US Department of Transportation
Federal Aviation Administration

Memorandum

DRAFT DRAFT DRAFT

Subject: **ACTION:** Advisory Material for FAR 33.5, 33.7, 33.27, 33.28, 33.29, 33.53, and 33.91 Affected by the Engine Harmonization Working Group (EHWG) Harmonization Effort.

Date: Sept. 26, 2000

From: Manager, Engine and Propeller Standards Staff, ANE-110

Reply to Attn. of: Cosimo Bosco
ANE-110
(781) 238-7118

To: Manager, Aircraft Engineering Division, AIR-100
Manager, Aircraft Manufacturing Division, AIR-200
Manager, Brussels Aircraft Certification Staff, AEU-100
Manager, Engine Certification Office, ANE-140
Manager, Engine Certification Branch, ANE-141
Manager, Engine Certification Branch, ANE-142
Manager, Boston Aircraft Certification Office, ANE-150
Manager, New York Aircraft Certification Office, ANE-170
Manager, Airframe and Propulsion Branch, ANE-171
Manager, Rotorcraft Directorate, ASW-100
Manager, Rotorcraft Standards Staff, ASW-110
Manager, Airplane Certification Office, ASW-150
Manager, Rotorcraft Certification Office, ASW-170
Manager, Special Certification Office, ASW-190
Manager, Small Airplane Directorate, ACE-100
Manager, Small Airplane Standards Office, ACE-110
Manager, Atlanta Aircraft Certification Office, ACE-115A
Manager, Propulsion Branch, ACE-140A
Manager, Chicago Aircraft Certification Office, ACE-115C
Manager, Propulsion Branch, ACE-118C
Manager, Wichita Aircraft Certification Office, ACE-115W
Manager, Propulsion Branch, ACE-140W
Manager, Anchorage Aircraft Certification Office, ACE-115N
Manager, Transport Airplane Directorate, ANM-100
Manager, Transport Standards Staff, ANM-110
Manager, Airframe and Propulsion Branch, ANM-112
Manager, Seattle Aircraft Certification Office, ANM-100S
Manager, Propulsion Branch, ANM-140S
Manager, Denver Aircraft Certification Office, ANM-100D
Manager, Los Angeles Aircraft Certification Office, ANM-100L
Manager, Propulsion Branch, ANM-140L
Deputy Director, Flight Standards Service, AFS-2
Manager, Air Transportation Division, AFS-200
Manager, Aircraft Maintenance Division, AFS-300
Manager, Flight Standards National Field Office, AFS-500
Manager, Aircraft Evaluation Group, Boston-AEG
Manager, Aircraft Evaluation Group, Ft Worth-AEG
Manager, Aircraft Evaluation Group, Missouri-Kansas City-AEG
Manager, Aircraft Evaluation Group, Long Beach, California-AEG
Manager, Aircraft Evaluation Group, Seattle-AEG

The purpose of this Program Memorandum is to provide advisory material for FAR paragraphs 33.5, 33.7, 33.27, 33.28, 33.29, 33.53, and 33.91 that have been modified because of the ARAC-Engine Harmonization Working Group (EHWG) harmonization effort for engine control systems. Subsequently, the FAA plan is to integrate this guidance material into AC 33-2B, Aircraft Engine Type Certification Handbook at its next update.

The Electronic Engine Control Task Group (EECTG) has been tasked by the Engine Harmonization Working Group (EHWG) to harmonize FAR 33.28 and JAR-E 50. Terms of Reference (TOR) have been issued that define the task to harmonize FAR 33.28 and JAR-E 50 for engine control systems. The FAR paragraphs for which this advisory material is provided have been modified as a result of the basic harmonization task for FAR 33.28 and JAR-E 50, although these FAR paragraphs are not noted in the TOR.

Advisory material for electronic engine controls (EEC) is provided by AC 33.28-1A that has been harmonized with AMJ-20X1. However, AC 33.28-1A is limited to electronic engine controls. The harmonization effort affected other paragraphs for which advisory material is required. This program memorandum is issued to provide guidance material for the paragraphs affected by engine control system harmonization effort and not covered under AC 33.28-1A.

Advisory material, referenced to paragraphs in AC 33-2B, is provided for the harmonized sections of the FAR as follows:

1. FAR 33.5 (Paragraph 17 of AC 33-2B) Instruction manual for installing and operating the engine.

a. Under (a) Installation Instructions, add paragraphs, as follows:

(1) ....

(2) .....

(3) .....

(4) A definition of the physical interfaces with the aircraft and aircraft equipment, including the propeller when applicable.

(5) Where a system certified with the engine relies on components which are not part of the engine type design, the system and interface requirements upon which engine type certification is based, or a reference to appropriate documentation containing these requirements, which is available to the installer.

(6) A list of the instruments needed for control of the engine, including the overall limits of accuracy and transient response required of such instruments to control operation of the engine.

b. Under (b) Operation Instructions, add the following paragraph, as follows:

(1)....

(2)....
(3)....
(4) A description of the operational modes of the engine control system and its functional interface with the aircraft systems, including the propeller when applicable.

c. Under Guidance, add the following paragraphs:

a.....

d.....

e. The engine instructions for installation should include or make reference to installation interface descriptions, limitations, and requirements of the engine control system. For example, the electronic engine control (EEC) power requirements and quality, including interrupt limitations, should be clearly defined for the installer. Another example is that the impedance and buffering limitations for the signals provided by the EEC system for display and instrumentation, or signals used by the EEC, such as air data information, should be specified.

f. The trend toward system integration may lead to EEC systems that:

(1) have other control functions integrated within the engine control system, such as an integrated engine and propeller control system or,

(2) depend on aircraft resources that form part of the engine certification basis.

Examples of these aircraft supplied resources include, recording of rotorcraft One Engine Inoperative (OEI) data and aircraft central computers that perform some or all of the engine control functions.

The engine applicant is responsible for specifying the requirements for the EEC system for these aircraft supplied resources in the engine instructions for installation and substantiating the adequacy of those requirements. However, responsibility for complying with the specified requirements lies with the installer.

g. The engine instructions for installation should include a description of all operational modes of the engine control system and its functional interface with the aircraft systems including backups or alternate modes whether dispatchable or not, and including the propeller when applicable.

2. FAR 33.7 (Paragraph 18 of AC 33-2B) Engine Ratings and Operating Limitations.

No additional guidance is required to address the addition of §33.7(d), because the regulatory language is sufficiently explicit.

3. FAR 33.27 (Paragraph 27 of AC 33-2B) Turbine, compressor, fan and turbosupercharger rotors.

The harmonization effort affects paragraph 27 in two ways. The regulatory language to require a protection means to preserve the structural integrity of the rotors is under two paragraphs as follows:

a.) 33.28(b)(3)(a), if provided by the engine control system, and,
b.) 33.27(b), if provided by other means.

The regulatory language of §33.27(b) has been modified to harmonize with the JAR requirements that provide other means of preserving the structural integrity of rotors, such as blade shedding and rotor interference means.

Paragraph 27 is changed as follows:

a.) Change the "Guidance" paragraph to be:

"The INTENT of this section is to assure engine rotor structural integrity, by design and functioning ***of a protection means that may include blade shedding or rotor interference techniques,*** to inhibit excedances.....without cracking. Protection means provided by the engine control system are addressed under §33.28(b)(3)(a)."

4. FAR 33.28 (This is a new paragraph for AC 33.2B.), Engine Control Systems
Section 33.28 Engine control systems:

Guidance. The intent of this section is to provide guidance for engine control systems implemented in technologies other than electrical/electronic technology. Guidance for electronic engine controls (EEC) systems is provided by AC 33.28-1A. The modification to AC 33.28-1 is a result of the harmonization effort conducted to harmonize of §33.28 and JAR E-50. This harmonization effort resulted in §33.28 being changed to apply to all engine controls, including hydromechanical controls or controls of other technology. The advisory material provided in AC 33.28-1A only applies to EEC systems although the rule has been changed to apply to all engine controls. Therefore, additional guidance material that applies to controls of other technology is provided in this policy memorandum and will subsequently be included in updated AC 33.2B.

(a) Applicability

§33.28 is applicable to all types of engine control systems. For instance, these might be hydromechanical control systems or hydromechanical control with a limited authority electronic supervisor control, single channel full authority engine control with hydromechanical back-up, dual channel full authority electronic engine control with no back-up, or any other combination. The electronic technology can be analog or digital.

The engine control system includes any system or device that controls, limits or monitors engine operation and is necessary for continued airworthiness standards of the engine. This covers all equipment that is necessary for controlling the engine and ensuring safe operation of the engine within its limits as specified in §33.28(a). This implies consideration of all control system components including the electronic control unit(s), fuel metering unit(s), variable-geometry actuators, cables, wires, sensors, etc.. The main engine fuel pump, which is usually engine-mounted and often physically integrated with the fuel metering unit, is not usually considered part of the engine control system.

These requirements cover the main engine control system as well as protection systems, for example, overspeed, over-torque or over-temperature.

When blade shedding or engine build related means is used for overspeed protection, this would not be considered under §33.28 as being part of the control system, as this protection is purely mechanical and will automatically work without influence from the engine control system. This type of protection is addressed under the requirements of §33.27(b).

Engine monitoring systems are covered by this section when they are physically or functionally integrated with the control system and they perform functions that affect engine safety or are used to effect continued-operation or return-to-service decisions. For instance, low cycle fatigue (LCF) cycle-counters for critical parts would be included but most trend monitors and propulsion multiplexers (PMUX) devices would not.

(b). Objective

For electronic engine control systems, AC33.28-1A, AC33-2B and this FAA Policy Memorandum provide additional and detailed interpretation of §33.28 with special consideration to interfaces with the aircraft, and the propeller when applicable.

The purpose of FAR-33.28 is to set objectives for the general design and functioning of the engine control system and these requirements are not intended to replace or supersede other requirements, such as §33.67 for the fuel system. Therefore, individual components of the control system, such as alternators, sensors, actuators, should be covered, in addition, under other part 33 paragraphs such as §33.53 and §33.91, as appropriate.

(c) Environmental Effects

The objective of §33.28(a)(2), in conjunction with §33.53 and §33.91, is to demonstrate that the engine control system can perform its intended function in its installed environment. Advisory material for HIRF, lightning and electromagnetic effects can be found in AC33.28-1A. Advisory material for environmental effects other than HIRF,

lightning and electromagnetic can be found in this program memorandum under advisory material for §33.91.

In particular, electronic engine control systems are sensitive to lightning and other electromagnetic interference and these conditions can be common to more than one engine.

For compliance with §33.28(a)(2), the functional integrity of the engine control system should be maintained when subjected to designated levels of electric or electromagnetic induction, including effects from external radiation and lightning. The environment, including radiated and conducted emissions, to which the engine control system and its components are qualified should be entered into the engine instructions for installation, and is considered to be an installation limitation for the installer. For aircraft certification, the aircraft manufacturer should substantiate that these levels are compatible with the installation.

When the installer specifies the environmental conditions of the installation, compliance with this requirement can be demonstrated by meeting the specified installation requirements.

When the installation requirements are not specified or not known, environmental conditions of a typical installation may be assumed.

It should be established by analysis or test that all components of the engine control system, including all electronics units, sensors, harnesses, hydromechanical elements, and any other relevant elements or units, operate properly in their declared environment. The environmental limits are not imposed by the rules, but should be representative of the environments that are expected to be encountered in the engine installation.

(d) Integrity

The intent of §33.28(b) is to establish engine control system integrity requirements consistent with operational requirements of the various applications. In particular, the introduction of electronic control systems should provide at least an equivalent level of safety and reliability for the engine as achieved by engines equipped with hydromechanical control and protection systems, and magneto systems. An analysis that demonstrates compliance with the requirements of §33.28(b) is required.

Mechanical and hydromechanical engine control systems rely on mechanical inspection intervals and "soft failure characteristics" to ensure control system integrity and airworthy operation between control system maintenance intervals.

The hardware of electronic control systems, however, tends to be characterised by random failures and does not lend itself to inspection for component wear. It is recognised that in order to achieve an upper limit on the LOTC rate consistent with the application,

electronic engine control systems should use redundancy and fault accommodation techniques to ensure safe and reliable control system operation following failure of electrical or electronic components. Paragraph (8) of AC33.28-1A provides additional material for electronic engine control systems.

§33.28(b) defines requirements for overspeed protection systems for the engine control system. Overspeed protection is normally provided in hydromechanical controls by flyball mechanisms. Although the functionally of these systems can not be assured by test before or after each flight, as are systems implemented by electronic means, it is still required that these overspeed systems be functional for each flight. This can be demonstrated through a test program that establishes the inspection or overhaul period that will ensure that the overspeed protection system will remain functional between the declared inspection or overhaul periods.

(e) Electrical Power

Engine control systems implemented in hydromechanical technology or technology other than electrical and electronic technology should inherently be compliant with §33.28(e). . However, if the system has functions implemented electrically or electronically that depend on aircraft-supplied electrical power, the system should be evaluated for compliance with this rule (see paragraph 13 of AC33.28-1A for relevant interpretation).

(f) Air Pressure Signals

§33.28(f) covers cases of ingress of foreign matter (e.g. sand, dust, water, or insects) which could result in blockage of the lines and result in an adverse effect on engine operation. For example, the experience has shown that lines used for measuring the static pressure in the compressor of turbine engines could be blocked by frozen water, leading to a loss of power. Precautions should therefore be taken, such as use of protected openings, filters, drains for water, heating of the lines to prevent freezing of condensed water. Corrosion effects should also be addressed.

It is required to minimize the effect because it is not possible to totally eliminate the threat. This should be done in light of the integrity requirements of §33.28(b), with due consideration to the fact that this could be an effect common to more than one engine on the same aircraft.

References

1.
2.
3.

5. FAR 33.29 (Paragraph 28 of AC 33.2B Instrument Connection).

a. Under **Paragraph 28, Section 33.29 Instrument connection** add paragraphs (d), (e) and (f) as follows:

(a.).....
(b.).....
(c.).....

(d.) Provision must be made for the installation of instrumentation necessary to ensure operation in compliance with engine operating limitations. When presenting the failure analysis, or complying with any other requirement, if dependence is placed on instrumentation which is not otherwise mandatory in the assumed aircraft installation, then this instrumentation must be specified in the engine instructions for installation and declared in the engine approval documentation.

(e) Means must be provided to minimize the possibility of incorrect fitting of instruments, sensors and connectors.

(f) The sensors, together with associated wiring and signal conditioning, must be segregated, electrically and physically, to the extent necessary to ensure that the probability of faults propagating vice versa, or from control functions to instrumentation and monitoring functions, is consistent with the criticality of the performed functions

b. Under **Guidance change to read as follows:**

The INTENT of this section is to prevent misconnections of engine-required instrumentation, and to provide a drawing location for rotor unbalance sensing. Additional guidance is provided for (d) and (f):

(d) Under the requirements of 33.29(d), the engine manufacturer should define the instrumentation which is necessary for engine operation within its limitations and also make provision for installation of this instrumentation.

(1) Paragraph 1305 of FAR 23, 25, 27 or 29 contains lists of powerplant instrumentation required for aircraft certification compliance. In addition, the engine failure analysis might show the need for specific instrumentation providing information to the flight crew or maintenance personnel for taking the appropriate actions in order to prevent the occurrence of a failure or to mitigate any associated consequences.

(2) Care should be exercised to ensure that the information (i.e., sensors and display system) provided to the flight crew is sufficiently representative, accurate and responsive for its intended function.

(3) If the safety analysis is dependent on instrumentation, assumptions regarding failure rates in any associated subsystems or elements, which are not part of the engine type design, should be specified (see FAR 33.75(d)).

(4) Care should also be exercised in selecting the position on the engine at which a particular parameter, such as oil pressure, is sensed in order to ensure that the indication is appropriate for the intended protection of relevant components.

(f) The intent of section 33.29 (f) is to provide for segregation of sensors, together with associated wiring and signal conditioning, to basically ensure that faults could not affect at the same time the monitoring functions and the engine control functions.

For example, if the inadvertent deployment of a reverser in-flight is critical to the aircraft, the thrust reverser position control and position indicating systems should be separate, such that failures which could effect the thrust reverser position control system are not allowed to cause loss of the correct flight deck indication of reverser position.

An example of a non-critical function in a multi-engine installation is the control of engine thrust or power. If the same sensor is used for engine control and indication, a malfunction of that sensor will affect both the indication and control of engine power or thrust. However, at the aircraft level, the power or thrust of one engine is not considered a critical function.

The level of segregation, and the associated probability of common fault, is dependent on the criticality of the considered functions.

6, FAR 33.53 (Paragraph 39 of AC 33.2B) Engine Component Tests.

Paragraph 39 is changed as follows:

a) Change the paragraph title and the bold section title from "Engine Component Tests" to "Engine System and Component Tests".

b) Change paragraph (a) of the rule to read as follows:

(a) For those systems or components which cannot be adequately substantiated by the endurance testing of FAR 33.49, additional tests or analyses must be conducted to demonstrate that the systems or components are able to perform the intended functions in all declared environmental and operating conditions.

c) Change "Guidance" to be as follows:

The intent of FAR 33.53 is to define the additional tests or analysis which would be necessary for those systems or components which are not necessarily tested during the endurance test of FAR 33.49.

(a) It is also recognized that the other requirements of FAR 33 do not always provide sufficient testing to cover all the conditions (pressure, temperature, vibration, etc. ...) which could affect the airworthiness of a piece of equipment throughout the declared flight envelope and within all the declared installation conditions.

(b) Other reasons for testing under 33.53 include, but are not limited to, the following examples:

- When testing is required in support of 33.28(a) validation throughout the declared flight envelope and within all the declared installation conditions.
- When a pressure relief valve in a turbo-supercharger is untested during the scheduled test of FAR 33.49.
- When an engine electronic control system has a mechanical back-up which is not normally used during the endurance test.
- When demonstration that a failure indicating system, on which dependence is placed in the engine safety analysis, will function satisfactorily when required.

(c) The Engine manufacturer should define, in agreement with the Authority, all necessary testing and / or analysis for those accessories or systems that need specific substantiation, in addition to the certification tests performed on a complete Engine, with attention paid to their location and operating conditions. Unless it is necessary to test the functioning of a system itself, substantiation of individual components can be made separately from the system they are part of.

5. FAR 33.91 (Paragraph 62 of AC 33.2B) Engine System and Component Tests.

Section 33.91 Engine system and component tests.
The following changes are made to paragraph 62;

a) Change the section title in both places to be "Engine System and Component Tests"
b) Change the rule to read as follows:

33.91 Engine Systems and Components Tests

(a) For those systems or components which cannot be adequately substantiated by the endurance testing of FAR 33.87, additional tests or analyses must be conducted to demonstrate that the systems or components are able to perform the intended functions in all declared environmental and operating conditions.

c) Change "Guidance" to be as follows:

The intent of FAR 33.91 is to define the additional tests or analysis, which would be necessary for those systems or components which are not necessarily tested during the endurance test of §33.87.

(1) It is also recognized that the other requirements of FAR 33 do not always provide sufficient testing to cover all the conditions (pressure, temperature, vibration, etc....) which

could affect the airworthiness of a piece of equipment throughout the declared flight envelope and within all the declared installation conditions.

Other reasons for testing under 33.91 include but are not limited to the following examples:

- When testing is required in support of 33.28(a) validation throughout the declared flight envelope and within all the declared installation conditions.

- When, for example, an overspeed protection system (or a torque limiter) is unlikely to be tested during the scheduled tests of FAR 33.87.

- When an engine electronic control system has a mechanical back-up which is not normally used during the endurance test.

- When demonstration that a failure indicating system, on which dependence is placed in the engine safety analysis, will function satisfactorily when required.

The Applicant should define, in agreement with the Authority prior to the start of testing, all necessary testing and / or analysis for those accessories or systems that need specific substantiation, in addition to the certification tests performed on a complete Engine, with attention paid to their location and operating conditions. Unless it is necessary to test the functioning of a system itself, substantiation of individual components can be made separately from the system they are part of.

The Applicant should define, in agreement with the Authority prior to the start of testing, all necessary conformity for both the hardware and the test setups. Conformity should be documented as part of the Certification Report. Differences between the test hardware and the type design hardware should be reviewed and approved by the Authority prior to the start of testing and included as part of the reconciliation in the Certification Report.

(2) The manufacturer should consider the applicability of the items listed in the Tables 1 to 4 below which are considered as being a guide. Additional guidance for EMI, HIRF and lightning is provided in AC 33.28 for all electrical/electronic components or components with electrical/electronic sub-components.

Consideration of general conditions such as those of RTCA DO 160 allows certification of components in a consistent manner, independently from any installation consideration. Nevertheless, the considered conditions must be shown to encompass the particular conditions specific to the declared installation. Documents that provide acceptable test procedures for each item are referenced in the same table. Other acceptable appropriate test and analysis procedures may be defined by the applicant. Compliance is normally demonstrated by test or analysis unless the component is shown to be sufficiently similar to and operates in an environment which is the same or less severe than previously certified components for which similarity is claimed.

The intent and applicability of each item of Tables 1 to 4 are also specified after each table.

The following list of applicable requirements and the associated tests or procedures (or their equivalent) has been accepted for evaluating component airworthiness. FAA approval of these environmental test plans should be obtained prior to commencing the tests.

(a) General Environmental Conditions

The following environmental conditions should be considered for all components.

Table 1

	ENVIRONMENTAL CONDITIONS	ACCEPTABLE TESTS/PROCEDURES
1	High Temperature Demonstration	EUROCAE ED-14 / RTCA DO-160, section 4 or Mil-E-5007 paragraph 4.6.2.2.5
2	Low Temperature Demonstration	EUROCAE ED-14 / RTCA DO-160, section 4 or Mil-E-5007 paragraph 4.6.2.2.7
3	Room Temperature Demonstration	EUROCAE ED-14 / RTCA DO-160, section 4 or Mil-E-5007 paragraph 4.6.2.2.6
4	Contaminated Fluids	As a reminder. See FAR requirements 33.67, 33.71, 33.66 for fuel/oil/air requirements. Mil-E-5007 paragraph 4.6.2.2.6 (fuel test only)
5	Vibration	EUROCAE ED-14 / RTCA DO-160, Section 8
6	Impact	EUROCAE ED-14 / RTCA DO-160, Section 7
7	Sustained Acceleration	EUROCAE ED-14 / RTCA DO-160, Section 7 or MIL-STD-810E, Method 513
8	Sand and Dust	EUROCAE ED-14 / RTCA DO-160, Section 12, Category D or MIL-STD-810
9	Fluid Susceptibility	EUROCAE ED-14 / RTCA DO-160, Section 11, Category F

10	Salt Spray	EUROCAE ED-14 / RTCA DO-160, Section 14, Category S / MIL-STD-810
11	Fuel System Icing	As a reminder. See FAR 33.67
12	Induction Icing	As a reminder. See FAR 33.68 & 33.35
13	Fungus	EUROCAE ED-14 / RTCA DO-160, Section 13, Category F
14	Temperature and Altitude	EUROCAE ED-14 / RTCA DO-160, Section 4

High Temperature Demonstration :

The high temperature demonstration is to verify that the component can function properly in its maximum temperature environment and to identify any damage caused by exposure to maximum temperature that could lead to component failure. Maximum conditions must take into account both ambient and external and internal fluids to which the component is exposed. Historical requirements can be found in MIL-E-5007 Paragraph 4.6.2.2.5. For electrical components with no mechanical elements (EUROCAE ED-14 /RTCA DO-160 Section 4) tests have been used to show compliance.

Low Temperature Demonstration :

The low temperature demonstration is to verify that the component can function properly in its minimum temperature environment and identify any damage caused by exposure to minimum temperature that could lead to component failure. Minimum conditions must take into account both ambient and external and internal fluids to which the component is exposed. Historical requirements can be found in MIL-E-5007 Paragraph 4.6.2.2.7. For electrical components with no mechanical elements (EUROCAE ED-14 /RTCA DO-160 Section 4) tests have been used to show compliance.

Room Temperature Demonstration :

The room temperature demonstration is to identify any damage caused by extended operation at room temperature that could lead to component failure. EUROCAE ED-14 / RTCA DO-160, section 4 tests have been used to show compliance. Historical requirements can be also be found in MIL-E-5007 Paragraph 4.6.2.2.6. This test may be combined with the contaminated fluids test, if applicable.

Contaminated Fluids:

The contaminated fluids requirement is to verify that the engine systems can function properly in a contaminated fluid environment. This can be achieved either by system testing or individual component test/analysis. Refer to the applicable FAR 33 requirements, such as Far 33.67 for fuel, FAR 33.71 for oil, and FAR 33.66 for air, for more details. Testing may be combined with room temperature demonstration.

Vibration :

The vibration requirement is to verify that exposure to the declared vibration environment does not cause structural failures and to verify that the component functions properly when exposed to that vibration. This can be addressed by either a specific unbalanced engine test or by component test. The component may not be required to be operational during component testing if the applicant can demonstrate by other means that the component operates satisfactorily or does not adversely impact system operation when

subjected to the declared vibration environment. EUROCAE ED-14 / RTCA DO-160, Section 8 tests are appropriate if the component vibration environment can be correlated to the DO 160 standards.

Impact :

The impact requirement is to verify that exposure to a specified level of impact does not cause structural failure. EUROCAE ED-14 / RTCA DO-160, Section 7 tests are appropriate. It may be possible to demonstrate compliance with an installation environment requiring operational shocks and crash safety testing through other tests conducted on the engine, such as blade-out tests, for example.

Sustained Acceleration :

The sustained acceleration requirement is to verify that exposure to sustained acceleration experienced during aircraft operations do not cause structural failure and verify that the component functions properly during and after exposure to sustained acceleration. EUROCAE ED-14 / RTCA DO-160, Section 7 are appropriate.

Sand and Dust :

The sand and dust requirement is applicable to all components that are not environmentally sealed. Testing should be performed according to EUROCAE ED-14 / RTCA DO-160 section 12, category D.

Fluid Susceptibility :

The fluid susceptibility requirement is to verify that the component can function properly after exposure to specified fluids and identify any damage caused by such exposure that could lead to component failure. Normally the fluids to be considered are those likely to be encountered in service, such as fuel, oil, hydraulic fluids, cleaning solvents, etc. Component testing may follow the procedures defined in EUROCAE ED-14 / RTCA DO-160 section 11, category F, paragraph 11.4.1 (Spray Test). At the conclusion of the test, the unit under test should be opened and inspected for entry of the test fluid. If evidence of fluid entry is detected the applicant should provide the rationale for accepting the test results based on the criticality of the quantity and location of the fluid entry point.

Salt Spray :

The salt spray requirement is to verify proper component operation after exposure to a salt spray environment. For environmentally sealed components, the requirement may be substantiated by an analysis that shows that the component external materials are immune to a salt spray environment. Testing may be performed according to EUROCAE ED-14 / RTCA DO-160 sections 14, category S.

Fuel System Icing :

Fuel system components normally substantiate their capability to operate in icing environment through system test or analysis.

Induction Icing :

Components exposed to engine gas path or bleed system icing normally substantiate their capability to operate in icing environment through an engine test or analysis.

Fungus :

The fungus requirement is substantiated by test or an analysis which shows that no materials which support the growth of fungus are used in the component. Testing may be performed as defined in EUROCAE ED-14 / RTCA DO-160, section 13.0, category F, (Fungus Resistance).

Temperature and Altitude:

The purpose is to verify by test or an analysis that the component operates per design intent through out the engine flight envelope. Testing may be performed as defined in EUROCAE ED-14 / RTCA DO-160, section 4.0,

(b) General Environmental Conditions for Electrical /Electronic Components.

The following environmental conditions should be considered for all electrical/electronic components or components with electrical/electronic sub-components. Additional advisory material on EMI, HIRF and lightning may be found in AC 33.28–1A.

Table 2

	ENVIRONMENTAL CONDITIONS	ACCEPTABLE TESTS/PROCEDURES
15	Thermal Cycle	EUROCAE ED-14 / RTCA DO-160, Section 5
16	Explosion Proofness	EUROCAE ED-14 / RTCA DO-160, Section 9
17	Humidity	EUROCAE ED-14 / RTCA DO-160, Section 6 / MIL-STD-810
18	Waterproofness	EUROCAE ED-14 / RTCA DO-160, Section 10 / MIL-STD-810 (RAIN)
19	EMI, HIRF & lightning	See AC 33.28-1A
20	Power Input	EUROCAE ED-14 / RTCA DO-160, Section 16 and 17/ MIL-STD-704

Thermal Cycle :

The thermal cycle requirement is to demonstrate that a component will continue to operate and not fail or be damaged when exposed to temperature cycles and thermal transients consistent with the declared temperature environment. Component testing may

follow the procedures defined in EUROCAE ED-14 / RTCA DO-160, Section 5. Unless other substantiating data is provided, a minimum of 10 thermal cycles should be considered for temperature variation. If the component has electrical sub-components, testing of the sub-components only may be acceptable.

Explosion Proofness:

The explosion proof requirement is to verify that a component cannot cause an explosion of flammable fluids or vapors. If applicable, explosion proof testing may be performed as defined in EUROCAE ED-14 / RTCA DO-160, section 9 (Explosion Proofness). Section 9 of DO-160 is applicable for demonstrating compliance with §33.28 and §33.91. Environment I defines equipment mounted in fuel tanks or within fuel systems. Environment II is an atmosphere in which flammable mixtures can be expected to occur as the result of a "fault causing spillage or leakage".

For installations in a Fire zone, the Fire zone will have extinguishing provisions, so that the explosion proof test given by Environment II of DO-160, section 9 is adequate. However, Flammable Fluid Leakage (FFL) areas may not have fire extinguishing provisions or any of the other safety requirements associated with Fire zones based on the assumption that there are no ignition sources in these areas. In these cases the explosion proof test given by **Environment I** of DO-160, section 9 may be required for aircraft installation. The applicant should note in the installation for instructions which environmental test has been conducted. Unless Environmental I testing has been conducted, the applicant should alert the installer in the installation for instructions that the equipment may be an ignition source.

Humidity :

The humidity requirement is to demonstrate that the component is not adversely effected, operationally or structurally, by ingress of moisture. Testing may be performed according to EUROCAE ED-14 / RTCA DO-160 section 6,

Waterproofness :

The water requirement is to verify that the component can function properly after exposure to water and identify any damage caused by water exposure that could lead to component failure. Water testing may be performed according to EUROCAE ED-14 / RTCA DO-160 section 10, Category S. Following the test, the unit under test should be opened and inspected for entry of water. If evidence of water entry is detected, the applicant should provide the rationale for accepting the test results based on the criticality of the quantity and location of the water entry point.

Power Input :

The power input requirement applies only to electrical/electronic components or components with electrical/electronic sub-components that receive power directly from the aircraft (e.g., EEC, HMU fuel shutoff solenoid). The purpose of this test is to demonstrate that such components can accommodate the full range of power inputs

declared for the installation. For applicable components, requirement may be substantiated by the test defined in EUROCAE ED-14 / RTCA DO-160, section 16.

(c) Mechanical Components

Other requirements of FAR 33 may affect some components as follows.

Table 3

	SUBJECT	ACCEPTABLE TESTS/PROCEDURES
21	Proof Pressure	FAR 33.18
22	Burst Pressure	FAR 33.18
23	Pressure Cycling Test	FAR 33.18
24	Fire	FAR 33.17 [Note: The engine control system must comply with 33.17(e)]

The related AC 33.17–1 and AC 33.18-1 are therefore relevant.

(d) Specialized Component Testing

Table 4

Specialized Component Testing	SUBJECT	ACCEPTABLE TESTS/PROCEDURE
25 Engine electronic control systems	Overheat	FAR 33.28 (b)(1)(iii)

Overheat:

The purpose of this test or analysis is to verify that the electrical/electronic portions of the engine control system, when subjected to an overheat condition leading to failure, will not cause a hazardous engine effect. See also AC 33.28-1A. If an overheat test/analysis is not completed, this must be declared as an installation limitation in the engine installation instructions and the consequences of an overheat should be addressed at aircraft certification.

h:\ehwg\finaldoc\totaeig\PM_6.doc

End of file.

U.S. Department of Transportation

Federal Aviation Administration

Advisory Circular

DRAFT-------- DRAFT DRAFT

Subject: COMPLIANCE CRITERIA FOR 14 CFR §33.28, AIRCRAFT ENGINES, ELECTRONIC ENGINE CONTROL SYSTEMS.

Date: October 10, 2000
Initiated By:
Cosimo Bosco, ANE-110

AC No: 33.28
Change:Rev. 1A
Version 9b

(3328ac9b.doc)

AC33.28-1A supercedes AC33.28-1.

AC33.28-1A has been harmonized with revised AMJ 20X-1 (Certification of Aircraft Propulsion Systems Equipped with Electronic Engine Control Systems) as part of the terms of reference (TOR) issued by the Engine Harmonization Working Group (EHWG) to the Electronic Engine Control Task Group (EECTG) to harmonize FAR33.28 and JAR E-50. This activity is part of the overall ARAC effort to harmonize the JARs and FARs..

Harmonization of §33.28 and JAR E-50 resulted in a change in §33.28 to apply the rule to all types of engine controls, including hydromechanical controls. Because both AC33.28-1 and AMJ 20X-1 provide advisory material dedicated to electronic engine control systems, it was decided to keep these documents dedicated to electronic engine control systems and to provide additional guidance material applicable to engine control systems implemented in other than electronic technologies. This additional advisory material is provided in an FAA policy memorandum that subsequently will be included in AC33.2B, Aircraft Engine Type Certification Handbook at the next update of this advisory circular.. The policy memorandum is harmonized with the corresponding ACJ advisory material from the JAR.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

AC 33.28-1A version 9b dated 10 Oct 2000 .

TABLE OF CONTENTS.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

1. PURPOSE. This Advisory Circular (AC) provides guidance and acceptable methods, but not the only methods, that may be used to demonstrate compliance with the regulations of Title 14 of the Code of Federal Regulations (14 CFR), part 33 section 33.28. Like all AC material, this AC is not, in itself, mandatory and does not constitute a regulation. While these guidelines are not mandatory, they are derived from extensive Federal Aviation Administration (FAA) and industry experience in determining compliance with the pertinent regulations.

The existing regulations for engine certification may require specific interpretation for engines equipped with electronic control systems with special regard to interface with the certification of the aircraft, and propeller when applicable. Because of the nature of this technology it has been considered useful to prepare advisory material specifically addressing the certification of these control systems.

This document discusses the compliance tasks relating to the engine, propeller and aircraft certification processes and indicates how these tasks could be allocated between the engine, propeller and aircraft manufacturers. It does not, however, seek to define or to interfere with the contractual arrangements made between the engine, propeller and aircraft manufacturers for the provision of any particular data.

2. SCOPE. This advisory material provides guidance on the interpretation and means of compliance with the relevant engine certification requirements for electronic engine control (EEC) systems, whether implemented in electrical and electronic, analog or digital technology. Additional guidance material is provided in interim policy memorandum , Advisory Material for FAR 33.5, 33.7, 33.27, 33.28, 33.29, 33.53, and 33.91 Affected by the Engine Harmonization Working Group (EHWG) Harmonization Effort dated [insert date] that will be integrated into the forthcoming update to AC33.2B.

It gives guidance on the precautions to be taken for the use of electronic technology for engine control and protection, limiting, and monitoring functions, and, where applicable, for integration of functions specific to an aircraft or a propeller. In the latter cases, this document is applicable to such functions integrated into the EEC system, but only to the extent that these functions affect compliance with FAR requirements.

Precautions have to be adapted to the criticality of the functions. These precautions may be affected by the degree of authority of the system, the phase of flight and the availability of a back-up system as defined in Section (7) of this AC.

3. RELEVANT REGULATIONS (CFR) AND REFERENCE DOCUMENTS.

a. Relevant Regulations (CFR). Sections 21.16, 33.4, 33.5, 33.17, 33.19, 33.27, 33.29, 33.49, 33.53, 33.75, 33.91(a), Appendix A of part 33, 23.901, 23.903, 23.1309, 25.901, 25.903, 25.939, 25.1181, 25.1309, 27.901, 27.903, 27.1309, 29.901, 29.903, 29.1309

b. Reference Documents (Advisory Circulars, Notices and Policy Letters/Memoranda).

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

(1) AC 20-115B, RTCA, Inc. Document RTCA/DO-178B, dated January 11, 1993 (AMJ 20-115B) RTCA Document RTCA/DO-178B/EUROCAE ED-12B).

(2) AC 20-136, Protection of Aircraft Electrical/Electronic Systems Against the Indirect Effects of Lightning, dated 3 May 1990 (SAE-AE4L 87-3 REV B dated October 1989).

(3) AC 20-53A, Protection of Aircraft Fuel Systems Against Fuel Vapor Ignition Due to Lightning, dated April 22, 1991.

(4) Federal Aviation Administration (FAA) Notice N8110.71, Guidance For The Certification of Aircraft Operating in High Intensity Radiated Field (HIRF) Environments, dated April 2, 1998.

(5) AC No. 21-16C (RTCA Document No. DO-160C) Environmental Conditions and Test Procedures For Airborne Equipment, dated February 14, 1990, and AC No. 21-16D (RTCA DO-160D/EUROCAE ED-14D) Environmental Conditions and Test Procedures for Airborne Equipment, dated July 21, 1998.

(6) Policy Memorandum, FAA Engine and Propeller Directorate Policy Regarding Time Limited Dispatch (TLD) Of Engines Fitted With Full Authority Digital Engine Control (FADEC) Systems, dated October 28, 1993.

(7) AC 33.2B Aircraft Engine Type Certification Handbook, dated June 30, 1993.

c. Industry Documents

(1) RTCA . DO-160D/EUROCAE ED14D, Environmental Conditions and Test procedures for Airborne Equipment, dated July 29, 1997.

(2) RTCA . DO-178B/EUROCAE ED12D, Software Considerations in Airborne Systems and Equipment Certification, dated December 1, 1992.

(3) SAE ARP 5107; Guidelines for Time-Limited-Dispatch for Electronic Engine Control Systems issued June 1997.

(4) SAE ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems issued November 1996.

(5) SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems issued December 1996.

(6) SAE ARP 926A/B Fault/Failure Analysis Procedure.

(7) SAE ARP 1834/A Fault/Failure Analysis for Digital Systems.

(8) RTCA DO-254/ EUROCAE ED-80 dated April 19, 2000.

d. Military Specifications.

(1) MIL-STD-461D, Requirements For the Control of Electromagnetic Interference Emissions and Susceptibility, dated January 11, 1993.

(2) MIL-STD-462D, Measurement of Electromagnetic Interference Characteristics, Test Standard For, dated February 5, 1996.

(3) MIL-STD-810E, Environmental Test Methods and Engineering Guidelines, dated July 31, 1995.

(4) MIL-HDBK-217F, Reliability Prediction of Electronic Equipment, dated February 28, 1995

(5) MIL-E-5007D Engines, Aircraft, Turbojet and Turbofan, General Specification For, dated October 15, 1973

4. PRECAUTIONS. The introduction of electronic technology can entail the following:

a. A greater dependence of the engine on the aircraft owing to the use of electrical power or data supplied from the aircraft,

b. A risk of significant failures common to more than one engine of the aircraft which might, for example, occur as a result of:

(i) Insufficient protection from electromagnetic disturbance (lightning, internal or external radiation effects), [see §33.28(a)(2)]

(ii) Insufficient integrity of the aircraft electrical power supply, [see §33.28(e)]

(iii) Insufficient integrity of data supplied from the aircraft, [see §33.28(d)]

(iv) Hidden design faults or discrepancies contained within the design of the propulsion system control software [see §33.28(c)], or

(v) Omissions or errors in the system/software specification. [see §33.28(c)]

Special design and integration precautions should therefore be taken to minimize these risks. One basic objective behind the rules of §33.28 is to keep the same independence of the engine from the aircraft as was provided with purely hydromechanical control systems for not aggravating an aircraft situation by adding a wrong behavior of the engine.

5. DEFINITIONS. The following definitions apply in the context of engine control systems for use of this AC.

Aircraft-supplied data means information which is generated in the aircraft systems and is used by the engine control system but whose source is not controlled under the

design authority of the engine certification applicant. This does not include inputs from those sensors which are used by, and normally dedicated to, the engine control system but which may be mounted in the airframe.

Alternate Control Mode means one mode where the operating characteristics or capabilities of the engine control are sufficiently different from the "primary mode" that the operating characteristics or capabilities of the aircraft, crew workload, or what constitutes appropriate crew procedures may be significantly impacted or changed.

Back-up system means a different type of system which is used as a stand by or alternate control mode to the primary or normal control mode or system.

Commercial and Industrial Grade Electronic Parts means commercial and industrial grade parts not manufactured to military standards.

Electronic Engine Control (EECS) System means the complete system which includes all the components necessary for the control of the power or thrust output of the engine, within the flight envelope and operating limitations.

Electronic Engine Control (EEC) Unit means the main electronic unit(s) of an electronic engine control system that usually includes the computing elements.

Fault or Failure means an occurrence which affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). Errors may cause failures, but are not considered to be failures.

Fault or Failure Condition means a condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

Fault or Failure Detection means the discovery of a fault or failure or the resulting condition.

Fault or Failure Accommodation means the capability of the engine control system or flight crew to mitigate, either wholly or in-part, the fault or failure.

Full Authority Digital Engine Control (FADEC) means an engine control system in which the primary functions are provided using digital electronics and wherein the electronic engine control (EEC) unit has full-range authority over the engine power or thrust.

Full-up System or Configuration means an EECS that has no faults or failures present, detected or undetected, which affect the control of engine power or thrust, engine

protection systems, indication of critical engine operating parameters or other safety features of the engine control system.

Loss of Thrust or Power Control (LOTC) means a condition where the control has lost the capability, due to control system failures or malfunctions, of governing the engine within the bounds contained in paragraph 8 of this AC.

Per hour means "per engine flight hour."

Primary Mode The mode of operation that is intended to be used for controlling the engine.This is often referred to as the "normal mode".

Programmed Logic Device means custom micro-coded components, such as Application Specific Integrated Circuits (ASIC) and Programmable Logic Devices (PLDs).

Uncovered Fault means a fault or failure for which either no detection mechanism exists or, if detected, no accommodation exists.

6. GENERAL. One of the objectives for the engine manufacturer in an engine certification program is to show that the certificated engine should be "installable" in a particular aircraft or aircraft type. It is recognized that the determination of compliance of the engine control system with applicable aircraft certification regulations will only be made during aircraft certification. . In the case where the application is unknown at the time of engine certification, the engine manufacturer should make reasonable installation and operational assumptions for the target application. Any installation limitations or operational issues will be noted in the instructions for installation or operation, and/or the Type Certification Data Sheet (TCDS).

When possible, co-ordination between the engine and the aircraft manufacturers is recommended in association with the relevant authorities as discussed under paragraph (16) of this AC.

7. SYSTEM DESIGN AND VALIDATION

(a) *Control Modes*

Under FAR 33(a)(1)(i) the applicant must perform all necessary testing and analysis to ensure that all control modes, including those which occur as a result of control fault accommodation strategies, are implemented as required.

All control modes, including alternative or back-up modes, should be capable of performing their intended functions in the environmental conditions, including HIRF and Lightning, declared in the engine instructions for installation. . "Performing their intended functions" means that the system functions within its specified limits throughout the declared operating conditions and flight envelope. It is assumed that the specified limits will result in a system that complies with Part 33 requirements. In some cases the agreed test plan(s) may allow for some transitory perturbations which are within the requirements for compliance with Part 33.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

In addition the requirement states that the system must comply with the specified operability requirements "....under all likely system inputs and allowable engine power or thrust demands....". This phrase means that the system should not limit the pilot inputs in order to comply with the operability requirements.

These rules and advisory material are not specifically intended to apply to any crew training modes. These modes are usually application, and possibly operator, specific and need to be negotiated on a case-by-case basis. However training modes should be described in the engine instructions for operation. Also precautions should be taken in the design of the control and its crew interfaces to prevent inadvertent entry into any training modes.

The need to provide protective functions, such as overspeed protection, for all control modes, including any alternative or backup modes, should be reviewed under the requirements of 33.28(b)(3) and 33.75.

For rotorcraft propulsion control systems with power turbine speed governing the requirement for modulation of engine power should be interpreted as the ability to progressively apply power as required to maintain power turbine speed within specified limits.

Any uncommanded power oscillations should be of such a magnitude as not to impact aircraft controllability in the intended application. In general, power oscillations less than 5% of normal maximum rated power at the flight condition may be considered acceptable. Regardless of the levels discussed herein, if the flight crew has to shutdown an engine because of unacceptable thrust or power oscillations, such an event would be deemed an in-service LOTC event.

§33.28(a)(1) primarily applies to the engine control system operating in its normal full-up configuration and to those alternative or back-up control modes for which the applicant wishes to take credit in his LOTC analysis for compliance with FAR 33.28(b). The engine control may have fault accommodation configurations or other operating modes that are safe, but transfer of operation into these modes or configurations would be normally classified as an LOTC event. Moreover, the applicant should provide assurance that operation in any such configurations will not result in an engine hazardous event, as defined in §33.75. All such configurations should be defined in the engine instructions for operation.

For control configurations where the applicant seeks to take credit in his LOTC analysis, but which are not intended to be dispatchable configurations, it may be acceptable to have specific operating limitations. In addition, compliance with 33.28(a)(1)(i) does not imply strict compliance with the operability requirements of §33.51, §33.65 and §33.73 in these non-dispatchable configurations, if it can be demonstrated that, in the intended application, no likely pilot control system inputs will result in engine surge, stall, flame-out or unmanageable delay in power recovery.

For example, in a twin-engined rotorcraft, a rudimentary back-up control may be adequate since frequent and rapid changes in power setting with the back-up control may not be necessary.

In addition to these operability considerations, other factors which should be considered in assessing the acceptability of such reduced-capability back-up control modes include :-

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

- The installed operating characteristics of the back-up mode and the differences from the primary mode. Consideration should be given to the likely impact on pilot workload, if the application is known, of any alternative control modes.
- The rate of transfer from the primary to the back-up mode (i.e. the reliability of the primary mode). Transfer rates of less than 1 per 20,000 hours have been considered acceptable.

Any limitations on operations in alternative or back-up modes should be clearly stated in the engine instructions for operation.

Descriptions of the functioning of the engine control system operating in its primary and any alternative modes should be provided in the engine instructions for installation and operation.

Early coordination between the engine manufacturer and the airframe manufacturer is recommended in order to ensure that the requirements for compliance with the appropriate airworthiness standards of CFR 14 Subchapter C are understood.

Performing some portion of the engine certification testing in the alternate or back-up mode(s), including transition between modes, can be used as part of the system validation required under §33.28(a)(1). However, analyses are generally required to substantiate that operating in the alternative or back-up modes has no affect on engine durability or endurance. As with the primary mode, demonstration of the durability and reliability of the control system in all modes is primarily addressed by the system or component testing of §33.91.

Engine Test Considerations - If the engine certification tests defined in FAR 33 are performed using only the primary full-up control system, it should be demonstrated, by analysis and/or test, that the engine can meet the defined test-success criteria when operating in any alternative or back-up control mode, if the alternate or back-up mode is considered dispatchable. This would be applicable to test requirements such as operability, blade-off, rain, hail, bird ingestion etc..

There may be some control modes which are not intended to be dispatchable, but for which LOTC credit is being sought, in which such capability may be lost. This may be acceptable provided that the safety assessment and the installation instructions reflect this loss of capability

Availability - If the applicant seeks to take credit in his LOTC analysis for a back-up control mode which is not normally exercised, then, in addition to meeting the above criteria, the availability of the back-up should be established by routine testing or monitoring to ensure that the back-up will be available when needed. The frequency of the testing should be approved by the certifying authority and documented in the instructions for installing and operating the engine.

(b) *Control Mode Transitions*

The intent of §33.28 (a)(1)(ii) is to ensure that any control mode changes, which occur as a result of control fault accommodation strategies, are implemented in an acceptable manner. "Unacceptable thrust or power oscillations" are defined in Section 7(a), above. "Other detrimental characteristics" as required in the rule include flameout, over temperature or over speed, for example, in addition to preventing surge and stall.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

In general, transition to the alternative mode should be accomplished automatically by the engine control system. However, systems wherein pilot action is required to engage the back-up mode may also be acceptable. For instance, a fault in the primary system may result in a "failed-fixed" fuel flow (constant power output) and some action is required by the pilot to engage the back-up system in order to modulate engine power.

The transient change in power or thrust associated with transfer to the alternate mode should be reviewed with the cognizant authority for compliance with 33.28(a)(1)(ii). Input from the installer should be considered. Although this is not to be considered a complete list, some of the items that should be considered when reviewing the acceptability of control mode transitions are:

- The frequency of occurrence of transfers to any alternate control mode and the capability of the alternate mode. Computed frequency-of-transfer rates should be supported with data from endurance or reliability testing, in-service experience on similar equipment, or other appropriate data.

- The magnitude of the power, thrust, rotor or propeller speed transients.

- Successful demonstration, by simulation or other means, of the ability of the engine control system to control the engine safely during the transition. In some cases, particularly those involving rotorcraft, it may not be possible to make a determination that the mode transition provides a safe system based solely on analytical or simulation data. Therefore, it may be advantageous to the applicant to propose a flight test program to support the data.

- For compliance with 33.28(a)(1)(ii), an analysis should be provided to identify those faults that cause control mode transitions either automatically or through pilot action.

- For helicopter or propeller applications, the transition should not result in excessive overspeed or underspeed of the rotor or propeller which could cause emergency shutdown, loss of electrical generator power or the setting-off of warning devices.

The power or thrust change associated with the transition should be declared in the instructions for installing the engine.

Time Delays - Any observable time delays associated with control mode transitions or in re-establishing the pilot's ability to modulate engine thrust or power should be identified in the engine instructions for operation. These delays would be assessed during aircraft certification.

Annunciation to the Flight Crew – If annunciation is required, the type of annunciation to the flight crew should be commensurate with the nature of the transition. For instance, reversion to a "supervisory" mode of control where the transition is automatic and the only observable changes in operation of the engine are different thrust control schedules, would require a very different form of annunciation to that required if timely action by the pilot is required in order to maintain control of the aircraft.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

The intent and purpose of the cockpit annunciation should be clearly stated in the engine instructions for installation. Early coordination between the engine manufacturer and the airframe manufacturer is recommended in order to ensure that the requirements are understood and that suitable provision is made in the airframe design.

(c) HIRF, lightning, and electromagnetic interference (EMI) system tests.
("Advisory Material for FAR 33.5, 33.7, 33.27, 33.28, 33.29, 33.53, and 33.91 Affected by the Engine Harmonization Working Group (EHWG) Harmonization Effort" dated 2000 is the program memorandum associated with this harmonization effort. It provides guidance for other environmental tests under the section dedicated to §33.91. The program memorandum will be integrated into AC33.2B, Aircraft Engine Type Certification Handbook at its next update. Environmental tests in accordance with MIL-STD-810E may be accepted in lieu of DO-160 tests where the MIL-STD-810E tests are equal to or more rigorous than those defined in DO-160.))

(i) Declared levels

When the installation is known, the engine control system during the engine type certification program should be tested at levels that have been determined and agreed by the engine and aircraft manufacturers. It is assumed that, by this agreement, the installation can meet the aircraft certification requirements. Successful completion of the testing to the agreed upon levels would be accepted for engine type certification. This, however, may make engine installability dependent on a specific aircraft installation.

If the aircraft application is not known or defined at the time of the engine certification, in order to determine the levels to be declared for the engine certification, the engine manufacturer may use the general threat defined at the aircraft level and use assumptions on installation attenuation effects.

If none of the conditions defined above is available, it is recommended that minimum default levels for system laboratory HIRF tests be as follows :

- For frequencies from 10 kHz to 700 MHz, a minimum test level should be 100 volts per meter average.

- For frequencies from 700 MHz to 18 GHz, the minimum test level should be 200 volts per meter average.

- For rotorcraft applications, the minimum test level should be 200 volts per meter average over the entire frequency range from 10 kHz to 18 GHz.

(ii) Test procedures.

(A) General

The installed engine controls system, including representative engine-aircraft interface cables, should be the basis for certification testing.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

EMI tests procedures and test levels conducted in accordance with MIL-STD-461/462 or DO-160 have been considered acceptable. However, when using MIL-STD-461/462 , if the two test procedures differ for a particular test case, the applicant should provide the rationale for conducting the test using the MIL-STD procedure rather than that of DO-160.

The applicant should use the HIRF test guidelines provided in Section 20 of RTCA / DO-160 / EUROCAE ED-14D or equivalent. However, it should be recognized that the tests defined in DO-160 are applicable at a component test level, requiring the applicant to adapt these test procedures to a system level HIRF test to demonstrate compliance with §33.28 (a)(2).

For lightning tests, the guidelines of AC 20-136 and Section 22 of DO-160 would be applicable. Pin Injection Tests (PIT) are normally conducted on the EEC unit and other system components as required. PIT levels are selected as appropriate from the tables of Section 22 of DO-160.

(B) Open loop versus Closed loop

HIRF, lightning, and EMI tests should be conducted as system tests on closed loop or open loop laboratory set-ups. The closed loop set-up is usually provided with hydraulic pressure to move actuators to close the inner actuating loops. A simplified engine simulation may be used to close the outer engine loop. Testing should be conducted with the engine control system controlling at the most sensitive operating point, as selected by the applicant. The system should be exposed to the HIRF, lightning, and EMI environmental threats while operating at the selected condition. There may be a different operating point for HIRF, lightning, and EMI environmental threats.

If the applicant elects to conduct tests in open loop set-ups, the following factors should also be considered :

- If special EEC test software is used, that software should be developed and implemented by guidelines defined for software levels of at least Level 2 in DO-178A, Level C in DO-178B, or equivalent. In some cases, the application code is modified to include the required test code features.

- The system test set-up should be instrumented to monitor both the output drive signals and the input signals.

- Anomalies observed on inputs or outputs should be duplicated on the engine simulation to determine whether the resulting power or thrust perturbations comply with the pass/fail criteria.

(iii) Pass/Fail Criteria

The pass / fail criteria for HIRF and lightning is that there should be "no adverse effect" on the functionality of the system.

The following are considered adverse effects :

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

- A greater than +/- 2 percent (+/- 10% for Small General Aviation applications) change of rated power or thrust change from the normal control governing capability for a period of more than one second.

- Transfers to alternate channels, backup systems, or reversionary modes.

- Component damage.

- Significant fault codes recorded in the fault memory.

- False fault annunciation to the crew which could cause unnecessary or inappropriate crew action.

- Erroneous operation of overspeed or thrust reverser circuits.

(iv) Component and Software Design Changes

Hardware or Software design changes implemented after initial qualification should be evaluated for their effects with respect to the EMI/HIRF and lightning environment. Appropriate testing and/or analysis should be defined to ensure that the original basis for certification is maintained. Component level testing may be acceptable for such purposes.

(v) Maintenance Actions

§33.4 requires that the applicant prepare Instructions for Continued Airworthiness (ICA). This includes a maintenance plan. Therefore, for any protection system that is part of the type design of the engine control system and is required by the system to meet the qualified levels of HIRF and lightning, a maintenance plan should be provided to ensure the continued airworthiness for the parts of the installed system which are supplied by the engine manufacturer.

The maintenance actions to be considered include periodic inspections or tests for required structural shielding, wire shields, connectors, and equipment protection components. The applicant should provide the engineering validation and substantiation of these maintenance actions.

(vi) Time Limited Dispatch (TLD) Environmental Tests

Although TLD is not a requirement for certification, HIRF and lightning tests for TLD are usually conducted together with tests conducted for certification. In order to gain approval for the use of TLD, applicants should demonstrate that dispatchable EEC configurations continue to meet the environmental requirements of the certification basis. For example, in some cases a single channel dispatch configuration is the worst case dispatch configuration and HIRF and lightning tests should be conducted on such a configuration to demonstrate compliance.

8. INTEGRITY OF THE CONTROL SYSTEM.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

AC 33.28-1A version 9b dated 10 Oct 2000 .

The intent of 33.28(b) is to establish engine control system integrity requirements consistent with operational requirements of the various applications. In particular, the introduction of electronic control systems should provide at least an equivalent level of safety and reliability for the engine - as achieved by engines equipped with hydromechanical control and protection systems, and magneto systems.

Mechanical and hydromechanical engine control systems rely on mechanical inspection intervals and "soft failure characteristics" to ensure control system integrity and airworthy operation between control system maintenance intervals.

The hardware of electronic control systems, however, tends to be characterized by random failures and does not lend itself to inspection for component wear. It is recognized that in order to achieve an upper limit on the LOTC rate consistent with the application, electronic engine control systems should use redundancy and fault accommodation techniques to ensure safe and reliable control system operation following failure of electrical or electronic components

1. Engine Control Design and Construction:
   A. General LOTC Guidance:
   The LOTC rate is the predicted number of LOTC events per engine flight hour. This predicted rate includes all single and combinations of control system failures or malfunctions that lead to LOTC events.
   (1) Definition of LOTC events and guidance on LOTC rates:
   (a) The following guidance is applicable to engine controls for FAA/JAA Part 23 installations complying with Part 25 propulsion requirements and Part 25 transport aircraft applications. For engines used in these applications, the electronic engine control (EEC) system should not cause more than one LOTC event per 100,000 engine flight hours. For these applications, an LOTC event is defined as one where:
   (i) the engine control system has lost the capability of modulating thrust or power between flight idle and 90% of maximum rated power or thrust at the operating condition, or
   (ii) the control system suffers a fault which results in a thrust or power oscillation greater than the levels given in Section 7 of this AC.
   (iii) the control has lost the capability to govern the engine in a manner which allows compliance with the operability requirements given in 33.65 and 33.73.

   (b) The following guidance applies to engine control systems intended for applications other than those defined in A.(1)(a) above:
   (i) Unless another LOTC rate is agreed (see paragraph (ii) below), the 1 per 100,000 hour LOTC rate defined above is still considered to be applicable, For these applications an LOTC event is as defined in paragraph 1.A.(1)(a) above; with the exception that the inability to meet the operability requirements of FAR 33.65 and 33.73 in the alternate or backup modes may not be included as LOTC events.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

Examples of engines in this category include turbine engines intended for rotorcraft applications. In general, the 100,000 LOTC rate is considered applicable for these engines, but the inability to meet the operability requirements of 33.67 and 33.73 in the alternate or backup mode(s) may not be part of the LOTC event definition. The following guidance applies to these applications:

- Single turbine engine rotorcraft: Single engine rotorcraft may be required to meet the operability requirements of 33.65 and 33.73 in the alternate or backup mode(s), unless the lack of this capability is demonstrated to be acceptable at the aircraft level. In general, if (1) the control transitions to the alternate or backup mode more frequently than the 100,000 LOTC rate,, and (2) normal flight crew activity requires rapid changes in power to safely fly the aircraft, then engine operability in the alternate or backup mode(s) is considered a necessity.
- Multi-turbine engined rotorcraft: For multi-engined rotorcraft, the LOTC definition may not need to include the inability to meet the operability requirements of 33.65 and 33.73 in the alternate or backup mode(s). This may be considered acceptable because when one engine control transitions to an alternate or backup mode that does not have robust operability, that engine can be left at a reasonably fixed or slowly modulated power condition. The engine(s) with the normally operating control(s) can change power – as necessary – to complete aircraft maneuvers and safely land the aircraft. Demonstration of the acceptability of this type of operation is considered aircraft certification issue.

(ii) The applicant may propose an LOTC criteria other than; (1) a 1 per 100,000 hour LOTC rate, or (2) the acceptability of not being compliant with the thrust or power oscillation levels given in AC 33.28(a)(1), or (3) the acceptability of not meeting the operability requirements of 33.65 and 33.73 in the alternate or backup mode, or any combination thereof, as the LOTC criteria for control system reliability and operability requirements. Such a proposal should be substantiated. The substantiation data should evaluate the criticality of the engine and control system relative to the intended application.

Examples of engines in this category are engines intended for small general aviation aircraft (i.e., less than 6,000 lbs. max takeoff gross weight): Based on an analysis of the current small general aviation aircraft fleet, it is considered acceptable to define an LOTC event as the inability of modulating thrust or power between flight idle and 85% of maximum rated power or thrust at all operating conditions, and an LOTC rate of 1 per 40,000 engine operating hours has been shown to represent an acceptable level of system reliability and safety.

The FAA will review applicant proposals and supporting data for using different acceptance criteria for the definition of an LOTC event and make

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

determinations of the acceptability of such proposals on a case-by-case basis. The intent is to show equivalence of the LOTC rate to existing systems in comparable applications. (For additional information, see 33.28(a)(1).)

(2) Control System LOTC Analysis:
A system reliability analysis should be submitted to substantiate the agreed LOTC rate for the control system.. A numerical analysis such as a Markov model analysis, fault tree analysis or equivalent analytical approach is expected.

The following guidance applies to LOTC analyses:

(a) The analysis should address all components in the system that can contribute to LOTC events. This includes all electrical, mechanical, hydromechanical, and pneumatic elements of the system. This should also include aircraft signals or data used by the engine control when the failure or malfunction of those signals or data can contribute to LOTC events. As discussed below, the analysis should also include failures and malfunctions which contribute to the transmission of incorrect information in the case where that incorrect information would lead to a flight crew initiated engine shutdown or thrust reduction to a level within the agreed LOTC definition. The fuel pump is generally not included. It is usually considered part of the fuel delivery system. As discussed in sub-paragraph (c)(1) of the advisory material for 33.28(d), the system definition includes those sensors or elements which may not be part of the engine type design, but which are dedicated to the system and contribute to LOTC events. An example of this is the throttle or power lever transducer, which is usually supplied by the installer. The reliability and interface requirements for these other than engine type design elements should be contained in the engine instructions for installation.

(b) The LOTC analysis should consider all fault types. This includes both covered and uncovered faults.

(c) Any periodic maintenance actions needed to find and repair both covered and uncovered fault conditions in order to meet the LOTC rate, should be contained in airworthiness limitations section of the engine Instructions for Continued Airworthiness.

(3) Guidance for the Failure Rates Used in the LOTC Analysis for any Commercial and/or Industrial Grade Electronic Components Used in the Control System:
The applicant should have in place plans for procurement, quality assurance, and process control for the vendor-supplied commercial and industrial grade electrical/electronic parts to ensure that the control system of the type design will continue to be provided at the reliability level which was considered during the engine certification and the component failure rates used in control system's LOTC analysis. When available and agreed by the authorities, the International Electrotechnical Commission Quality Assessment System for Electronic Components (IECQ) "Avionics Industry: Guide for Component Management" may be used for additional guidance.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

Commercial and industrial grade parts have typical operating ranges of 0 degrees to +70 degrees Celsius and -40 degrees to +85 degrees Celsius, respectively. (Military grade parts are typically rated at -54 degrees to 125 degrees Celsius.) Commercial and industrial grade parts are typically defined in these temperature ranges in vendor parts catalogs. If the declared temperature environment for the engine control system exceeds the stated capability of the commercial or industrial grade electronic components, the applicant should substantiate that

(a) the proposed extended range of the specified components is suitable for the application, and
(b) the failure rates used for those components in the LOTC analysis are appropriately adjusted for the extended temperature environment.

When any electrical or electronic components are changed, the SSA and LOTC analyzes should be reviewed with regard to the impact of any changes in component reliability. Component, subassembly or assembly level testing may be required by the Authorities to substantiate that a change that introduces a commercial or industrial part(s) does not change the certification basis of the engine control system.

In some applications, it may be acceptable to use components classified as Automotive Parts. The guidance provided above is applicable to these parts as well.

B. Effects of Single Electrical/Electronic Component Failures on the LOTC Rate: Compliance with the single fault requirements of 33.28(b)(1)(ii) may be substantiated by a combination of tests and analyses. The intent of 33.28(b)(1)(ii) is that the engine control system be "essentially" single fault tolerant of electrical/electrical component failures.

It is recognized that to achieve complete single fault tolerance could require a triplicated design approach or a design approach with 100% fault detection. Currently, systems have been designed with dual, redundant channels or with backup systems that provide what has been called "essentially single fault tolerant". Although these systems may have some faults that are not covered, they have demonstrated excellent in-service safety and reliability, and have proven to be acceptable.

The objective, of course, is to have all the faults covered, and the dual channel or backup system configurations do cover the vast majority of potential electrical and electronic faults. However, on a case-by-case basis it may be appropriate for the applicant to omit some coverage because detection or accommodation of some electrical/electronic faults may not be practical. In these cases, the certification authorities recognize that single, simple electrical or electronic components or circuits can be employed in a reliable manner, and that requiring redundancy in some situations may not be appropriate. In these circumstances, failures in some single electrical or electronic components, elements or circuits may result in an LOTC event. This is what is meant by the use of the term "essentially", and such a system may be acceptable.

Single electrical and electronic faults that result in LOTC events should be identified and reviewed with the authority.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

C. Contribution of Single Electrical/Electronic Component Failures to Hazardous Events: Compliance with the single fault requirements of 33.28(b)(1)(iii) may be substantiated by a combination of tests and analyses. The intent of 33.28(b)(1)(iii) is that single electrical/electrical component failures in the engine control system should not result in a hazardous engine event as defined in FAR 33.75. In addition, the aircraft should not be dispatched if it is known that an engine control system provided protective feature is not available, such that a single electrical or electronic failure in the control system could result in a hazardous engine event.

D. Local Events

When the installation environment is more severe than the declared environmental limits, the LOTC requirements of 33.28(b)(1)(i) are not applicable. The applicable requirement for operation in a severe environment is that control system failures shall not result in a hazardous engine effect, as defined in FAR 33.75. Occurrence of severe environmental events would normally be limited to one engine and are referred to herein as "local events". A local event is not usually considered to be a common mode event, and common mode threats, such as HIRF, lightning and rain are not considered local events. (There may be installations where multiple engines are affected by the same local event. Such installations should be given consideration by the engine manufacturer and will be reviewed at aircraft certification.)

(1) Examples of local events:

(a) Fluid leaks or mechanical disruptions which could lead to damage to control system electrical harnesses, connectors, or the control unit(s),

(b) Fires, and

(c) Overheat conditions, for example, those resulting from hot air duct bursts.

(2) Consideration of Local Events.

(a) Whatever the local event, the behavior of the electronic engine control (EEC) system should not cause a hazardous engine effect, as defined in FAR 33.75.

(b) When demonstration that there is no hazardous engine condition is based on the assumption that there exists another function to afford the necessary protection, it should be shown that this function is not rendered inoperative by the same local event on the engine (including destruction of wires, ducts, power supplies).

(c) For the purposes of the rule, it is considered that an overheat condition exists when the temperature of the system components is greater than the maximum design operating temperature for the components - as declared by the engine manufacturer in the engine instructions for installation. The electronic portions of the control system should not cause a hazardous engine condition when the electronic components or units of the system are exposed to a continuous overheat or over-temperature condition. Specific design features or analysis

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

methods may be used to show compliance with respect to the prevention of hazardous effects. Where this is not possible, for example, due to the variability or the complexity of the failure sequence, then testing may be required.

(d) The electronic engine control system, including the electrical/electronic and mechanical parts of the system, must comply with the fire requirements of FAR 33.17 and the interpretative material of AC 33.17 is relevant. This rule applies to the elements of the engine control system which are installed in designated fire zones.

(e) There is no probability associated with 33.28 (b)(1)(iv). Hence, all foreseeable local events should be considered. It is recognized, however, that it is difficult to address all possible local events in the intended aircraft installation at the time of engine certification. Therefore, sound engineering judgement should be applied in order to identify the reasonably foreseeable local events.

Each wire interfacing with the electronic control unit should be tested or analyzed with respect to wiring faults. These faults should include opens and shorts to ground, and the test or analysis should show that the fault results in an identified and non-hazardous engine response.

Engine control unit aircraft interface wiring should be tested or analyzed for shorts to aircraft power, and these "hot" shorts should result in an identified and non-hazardous effect, as well. Where aircraft interface wiring is involved, the installer should be informed of the potential effects of wiring faults on aircraft interface wiring in the engine instructions for installation. It is the installer's responsibility to ensure that there are no wiring faults which could affect more than one engine, and if practical, more than one FADEC channel of a single engine by isolation/separation of the relevant wiring/conductors.

Where physical separation of conductors is not practical, coordination between the engine manufacturer and the installer should ensure that the potential for common mode faults between engine controls is eliminated, and between channels on one engine is minimized.

(f) The applicant should assess by analysis or test the effects of hydraulic or lubricating leaks impinging on components of the electronic engine control system. Such conditions should not result in a hazardous engine effect, nor should the fluids be allowed to impinge on circuitry or printed circuit boards and result in a potential latent failure condition. Refer to the Advisory Material for FAR 33.91 for test procedures with regard to fluid susceptibility.

E. Engine Control System Shared Signals:
The failure or corruption of data or signals originating within an engine control system and shared across engines should not cause an unacceptable change in thrust or power. This subject is discussed in the Safety Assessment advisory material in section 2 below.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

9. SYSTEM SAFETY ASSESSMENT

The system safety assessment (SSA) required under FAR 33.28 (b) (2) should address all operating modes, and the data used in the SSA should be substantiated.

The SSA should consider faults and their effects on the engine control system and the engine itself. The intent is to primarily address the faults or malfunctions which only affect one engine control system, and therefore only one engine. However, faults in aircraft signals in a multi-engined installation that could affect more than one engine should also be included in the SSA. These types of faults are addressed under 33.28(d).

The engine control SSA and LOTC analyses should identify the applicable assumptions, installation requirements and any control system limitations. The assumptions, installation requirements, and any limitations relating to control system operation should be stated in the engine instructions for installation, and if necessary, the limitations should be contained in the airworthiness limitations section of the instructions for continued airworthiness. This should include any periodic inspections and repair requirements for control system components.

A. Scope of the Assessment:
The SSA should address all Hazardous and Major effects identified under FAR 33.75 and also should include, but not necessarily be limited to, the following events caused by engine control system malfunctions:

(1) Failures affecting power or thrust and resulting in LOTC events (i.e., the LOTC analysis)
(2) Failures which result in the engine's inability to meet the operability requirements of 33.65 and 33.73. (If these are not LOTC events, document the expected frequency of occurrence for these events. The acceptability of the frequency of occurrence for these events – along with any aircraft flight deck indications deemed necessary to inform the flight crew of such a condition - will be determined at aircraft certification.)
(3) Transmission of erroneous parameters which could lead to thrust or power changes greater than 10% (e.g., false high indication of the thrust or power setting parameter) or to engine shutdown (e.g., high EGT or turbine temperatures or low oil pressure).
(4) Failures affecting functions included in the control system, which may be considered aircraft functions. Examples of these include, propeller control, TLD, thrust reverser control, etc.

The SSA should also consider all signals used by the control, including any cross-engine-control signals.

B. Pass/Fail Considerations:
Guidelines for the pass/fail criteria with respect to reliability requirements for the system safety assessment are as follows:

(1) Compliance with 33.75

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

(2) Failures leading to LOTC events: For control system failures or malfunctions leading to LOTC events, the control system has to have an average LOTC rate that is less than or equal to the agreed LOTC rate for the intended application. See paragraph 1.(A) of this AC.

(3) Failures affecting engine operability: If engine operability is included in the definition of LOTC events, then failures or malfunctions resulting in the engine's non-compliance with 33.65 and 33.73 should be contained in the LOTC analysis and need to be accounted in the agreed LOTC rate. If engine operability is not part of the LOTC definition, then the total frequency of occurrence of failures that result in engine response that is non-compliant with 33.65 and 33.73 requirements should be contained in the SSA and the acceptability of the frequency for these events – along with any aircraft flight deck indications deemed necessary to inform the flight crew of such a condition - will be determined at aircraft certification.

(4) Transmission of faulty parameters: The consequence of the transmission of a faulty parameter by the control system should be identified and included, as appropriate, in the LOTC analysis. Any information necessary to mitigate the consequence of a faulty parameter transmission should be contained in the engine operating instructions. For example, the engine's Operating Instructions may indicate that a display of zero oil pressure can be ignored in-flight if the oil quantity and temperature displays appear normal. In this situation, failure to transmit oil pressure or transmitting a zero oil pressure signal should not lead to an engine shutdown or LOTC events. Admittedly, flight crew initiated shutdowns have occurred in-service during such conditions. In this regard, if the engine operating instructions provide information to mitigate the condition, then control system faults or malfunctions leading to the condition do not have to be included in the LOTC analysis. In such a situation, the loss of multiple functions should be included in the LOTC analysis. For example, if the display of zero oil pressure and zero oil quantity (or high oil temperature) would result in a crew initiated shutdown, then those conditions should be included on the systems LOTC analysis.

(5) The criticality of functions included in the control system for aircraft level functions needs to be defined by the aircraft manufacturer.

C. Malfunctions or Faults Affecting Thrust or Power:
The engine control SSA should consider both undetected and detect faults and their effects on the control system and the engine.

Concerning the flight crews' capabilities for "detecting and reporting fault conditions" which result in engine power or thrust differences in a multi-engined aircraft: It is generally accepted that the flight crews may not note the engine operating differences when the difference is less than (approximately) 5% in thrust or power. For this reason thrust changes less than approximately 5% are generally considered undetectable by the flight crews. If a greater than 5% thrust difference occurs during a takeoff, the flight crews are likely to note the condition and may elect to abort the takeoff. Takeoff aborts at

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

low aircraft speeds are generally not considered a flight safety related event, but they certainly are undesirable.

The following guidance applies to undetected and detected malfunctions or faults which affect thrust or power. This guidance is particularly applicable to installations designed to meet Part 25 requirements. In some applications, the applicant may propose to the FAA other levels for some or all of the guidance provided below. The applicant should present substantiation why the proposed alternate levels are appropriate to the application being certificated.

(1) Undetected faults :

(a) When operating in the takeoff envelope, undetected or uncovered faults in the engine control system, which result in a thrust or power change of less than 3%, are generally considered acceptable).) However, this does not detract from the applicant's obligation to ensure that the full-up system is capable of providing the declared minimum rated thrust or power (i.e. such faults should be random in nature and detectable and correctable during routine inspections, overhauls or power-checks).

(b) When operating in the takeoff envelope, the frequency of undetected or uncovered faults or malfunctions that result in a thrust or power change greater than 3%, but less than the change defined as an LOTC event, should be contained in the SSA documentation. There are no firm requirements relating to this class of faults or malfunctions for engine certification, however the rate of occurrence of these types of faults should be reasonably low, like 10^{-4} events per engine hour or less. These faults may be required to be included in aircraft certification analysis.

(c) Signals sent from one engine control to another in an airplane application, such as signals used for ATTCS, , synchrophasing, etc., should be authority limited by the receiving control, so that undetected faults do not result in an unacceptable change in thrust or power on the engines using those signals.

(d) It is recognized that signals sent from one engine control to another in a rotorcraft application, such as load sharing and one engine inoperative (OEI)signals, can have a much greater impact on engine power when those signals fail. These failure effects should be contained in the SSA.

(2) Detected faults :

(a) When operating in the takeoff envelope, detected faults in the engine control system which result in a thrust or power change of up to 10%, may be acceptable if the total frequency of occurrence for these types of failures is relatively low. . The frequency of occurrence for this category of faults should be contained in SSA documentation. It should be noted that requirements for the allowable frequency of occurrence for this category of faults and any need for a flight deck indication of these conditions should be determined during aircraft certification. A total frequency of occurrence of less than 10^{-4} events per engine hour may be acceptable.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

(b) Detected faults in signals exchanged between engine controls should be accommodated so as not to result in an unacceptable thrust or power change on the engine using the cross-engine signals. For example, synchronizers should be limited in thrust or power authority.

10 PROTECTIVE FUNCTIONS

A. Rotor Overspeed Protection.
The intent of 33.28(b)(3) is to protect the rotating parts of the engine by providing "reasonable assurance" that the engine rotor speed limits will not be exceeded in service. Compliance with the "reasonable assurance" requirement of the rule is achieved by providing an independent overspeed protection system, such that it requires two independent faults or malfunctions (as described in 3.A.(1) below) to result in an uncontrolled overspeed. The following guidance applies if the rotor overspeed protection is provided by an engine control system function:

(1) In all dispatchable configurations, the overall engine system (i.e., the engine and overspeed protection system) must be at least two independent faults removed from an uncontrolled overspeed event. Hence, a potential rotor overspeed burst should only be possible as a result of a first fault causing an overspeed and an independent fault preventing the overspeed protection sub-system from operating properly.

(2) The SSA should show that the probability per engine flight hour of an uncontrolled overspeed condition from any cause in combination with a failure of the overspeed protection system to function is less than one event per hundred million hours (a failure rate of 10^{-8} events per hour). The applicant should be aware that due to the severity of an uncontained engine failure in some installations, the hourly rate for this combined event may have to be shown to be less than one event per billion hours (10^{-9}) for certification of the aircraft.

(3) The overspeed protection system would be expected to have a failure rate consistent with recent industry experience which is better than 10^{-4} failures per operating hour to comply with the overall objective.

(4) A self-test of the overspeed protection system to ensure its functionality prior to each engine start/stop cycle is normally necessary for achieving the objectives. Verifying the functionality of the overspeed protection system at engine shutdown of the previous flight is considered acceptable.

(5) With multiple path overspeed protection systems, there will always be uncertainty that all paths are functional at any given time. Where multiple paths can invoke the overspeed protection system, a test of a different path may be performed each engine cycle. As a means to achieve a reasonable assurance of availability of the function, the objective is that a complete test of the overspeed system is achieved in a minimum number of engine cycles. It is recommended that the control system should

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

not be considered dispatchable if the overspeed protection system has an instantaneous failure rate greater than 10^{-4} failures per operating hour.

(6) The applicant may provide data that demonstrates that the mechanical parts of the overspeed protection system can operate without failure between stated periods, and a periodic inspection may be established for those parts. This data may be considered in lieu of testing the mechanical parts of the sub-system each engine cycle. When this approach is used, the test conducted each engine cycle may be limited to the electrical and electronic components of the overspeed protection system.

(7) When the overspeed control function is implemented via mechanical or hydromechanical means only, such as a fly-ball governor system, a periodic inspection or test interval is acceptable for compliance with the requirement for "continued system availability". The periodic inspection or test interval should be based on test or in-service data that demonstrates that the system operates without failure between intervals.

4. Other Protective Functions.
The engine control system may perform other protective functions. Some of these may be engine functions, but others may be aircraft or propeller functions. Engine functions should be considered under the guidelines of this Advisory Material, AC33.28-1A. The integrity of other protective functions provided by the engine control should be consistent with a hazard assessment associated with those functions, but if those functions are not concerned with the engine or engine systems, they may not be a part of engine certification.

As engine controls become increasingly integrated into the aircraft and propeller systems, they are incorporating protective functions that were previously provided by the aircraft or propeller systems. Examples are:
-reducing the engine to idle thrust if a thrust reverser inadvertently deploys, and
-providing the auto-feather function for the propeller when an engine fails.

The reliability and availability associated with these functions should be consistent with the aircraft level hazard assessment of conditions involving these functions. This will be completed during the aircraft certification.

Hence, if for example, an engine failure with loss of the auto-feather function is catastrophic at the aircraft level - and the auto-feather function is incorporated into the engine control system - the applicant will have to show for Part 25 or Part 23 applications certified to Part 25 requirements that an engine failure with loss of the auto-feather function cannot result from a single control system failure, and that combinations of control system failures, or engine and control system failures, which lead to a significant engine loss of thrust or power with an associated loss of the autofeather function may be required to have an extremely improbable event rate (i.e., 10E-09 events per hour).

Although these functions await evaluation at the aircraft level, it is strongly recommended that if practicable, the aircraft level hazard assessment involving these functions be available at the time

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

of the engine control system certification. This will facilitate discussions and coordination between the engine and aircraft certification offices under the conditions outlined in paragraph 16 of this AC. It is recognized that this coordination may not occur for various reasons. Because of this, the applicant should recognize that although the engine may be certified, it may not be installable at the aircraft level.

11 SOFTWARE DESIGN AND IMPLEMENTATION

(a) Objective

For engine control systems that use software, the objective of §33.28(c) is to prevent as far as possible software errors that would result in an unacceptable effect on power or thrust, or other unsafe condition.

It is understood that it may be impossible to establish with certainty that the software has been designed without errors. However, if the applicant uses the software level appropriate for the criticality of the performed functions and uses an approved software development method, the Authorities would consider the software to be compliant with the requirement to minimize errors. In multiple engine installations, the possibility of software errors common to more than one engine control system may determine the criticality level of the software.

(b) Approved Methods

Methods for developing software, compliant with the guidelines of RTCA documents DO-178A/EUROCAE ED-12A and DO-178B/EUROCAE ED-12B, hereafter referred to as DO-178A and DO-178B, respectively, are acceptable methods. Alternative methods for developing software may be proposed by the applicant and are subject to approval by the authorities.

Software which is not developed using DO 178B is referred to as legacy software. In general, software changes made to legacy systems applicable to its original installation are assured in the same manner as the original certification. When legacy software is used in a new aircraft installation that requires DO-178B, the original approval of the legacy software is still valid, assuming equivalence to the required software level can be ascertained. If the software equivalence is acceptable to the authorities, the legacy software can be used in the new installation that requires DO-178B software. If equivalence cannot be substantiated, all the software changes should be assured using DO-178B.

(c) Level of software design assurance

In multiple engine installations, the design, implementation, and verification of the software in accordance with Level 1 (DO-178A) or Level A (DO-178B) is normally needed to achieve the certification objectives for independence of engines for aircraft to be type certificated under Part 25 transport, Part 23 Commuter, and Part 27, Category A and Part 29, Category A.

The criticality of functions on other aircraft may be different, and therefore, a different level of software design assurance may be acceptable.

Determination of the appropriate software assurance level may depend on the failure modes and consequences of those failures. For example, it may be the case that failures resulting in significant thrust or power increases or oscillations may be more severe than an engine shutdown, and therefore, the possibility of these types of failures should be considered when selecting a given software assurance level.

It may be possible to partition non-critical software from the critical software and design and implement the non-critical software to a lower level as defined by the RTCA documents. The adequacy of the partitioning method should be demonstrated. This demonstration should consider whether the partitioned lower software levels are appropriate for any anticipated installations. Should the criticality level be higher in subsequent installations, it would be difficult to raise the software level.

(d) Architectural Protection

As it is not possible to be certain that there are no software errors, the need for additional system protection, beyond reliance on a high level of discipline in the software development and certification methodology, in order to preclude an unsafe condition, should be derived from the system safety analysis required under §33.28(b).

(e) On-Board or Field Software Loading and Part Number Marking

The following guidelines should be followed when on-board or field loading of Electronic Engine Control software and associated Electronic Part Marking (EPM) is implemented.

For software changes, the software to be loaded should have been documented by an approved design change and released with an approved service bulletin.

Software loading procedures and loading equipment should have been previously approved.

The verification test program should demonstrate that the new software version is compatible with the loading system(s).

For those EEC Units having separate part numbers for hardware and software, the software part numbers need not be displayed on the unit as long as the software part number is embedded in the loaded software and can be verified by electronic means. When new software is loaded into the unit, the same verification requirement applies and the proper software part number should be verified before the unit is returned to service.

For those EEC Units having only one part number, which represents a combination of a software and hardware build, the unit part number on the nameplate should be changed when the new software is loaded. The software build or version number should be verified before the unit is returned to service.

The configuration control system for electronic engine control system that will be onboard/field loaded and using electronic part marking should be approved. The drawing system should provide a compatibility table that tabulates the combinations of hardware part numbers and

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

software versions that have been approved by the authorities. The compatibility table may either be combined with one of the hardware or software Line Replaceable Unit (LRU) drawings or it may be a separate drawing. The top-level compatibility table should be under configuration control, and it should be updated for each change that affects hardware/software combinations. The applicable service bulletin should define the hardware configurations with which the new software version is compatible.

The loading system should be in compliance with the guidelines of DO-178B, Section 2.5.

If the applicant proposes more than one source for loading, (e.g., diskette, mass storage, etc.), all sources should comply with these guidelines.

The service bulletin should require verification that the correct software version has been loaded after installation on the aircraft.

(f) Software Change Category

The processes and methods used to change software should not affect the design assurance level of that software. Per current policy, there is no minor change category for DO 178A Level 1 or DO 178B Level A software. Consequently, all changes to Level 1 or A software are considered "Major" and require that they be processed as a "Major Change to the Type Design".

(g) Software Changes By Other than the TC Holder

There are two types of potential software changes that could be implemented by someone other than the original TC holder:

- option-selectable software or
- user modifiable software (UMS).

Option selectable changes would have to be pre-certified logic utilizing a method of selection which has been shown not to be capable of causing a control malfunction.

UMS is software intended for modification by the aircraft operator without review by the certification authority, the airframe manufacturer, or the equipment vendor. If this is the case, the aircraft operator should demonstrate that the engine and its modified control system continue to meet all FAR-33 requirements for certification. For engine control systems, UMS has generally not been applicable. However, approval of UMS, if required, would be addressed on a case-by-case basis.

The necessary guidance for UMS is contained in DO-178B, paragraph 2.4. In essence, it conveys the position that other than TC holders may modify the software within the modification constraints defined by the TC holder, if the system has been certified with the provision for software user modifications. To certify an electronic engine control system with the provision for software modification by other than the TC holder, the TC holder should (1) provide the necessary information for approval of the design and implementation of a software change, and (2) demonstrate that the necessary precautions have been taken to prevent the user modification

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

from affecting engine airworthiness, whether the user modification is correctly implemented or not.

In the case where the software is changed in a manner not pre-allowed by the TC holder as "user modifiable", the "non-TC holder" applicant will have to follow the process given in FAR 21.

12. AIRCRAFT SUPPLIED DATA

(a) Objective

In case of loss, corruption or failure of aircraft-supplied data, the engine should continue to function in a safe and acceptable manner, without unacceptable effects on thrust or power, hazardous engine effects, or loss of ability to comply with the operating requirements of §33.51, §33.65 and §33.73. This is imposed only to the engines to be installed in a multi-engine installation. For single engine installations, the effects should be reviewed as part of the overall safety and reliability objectives of §33.28(b).

(b) Background

§33.28(d) retains the independence of engines from the aircraft, which has traditionally been the case for aircraft equipped with engines having hydromechanical control systems, while providing sufficient flexibility to accommodate the increasing engine and aircraft integration that accrues from the use of electronic technology.

The intent is for the engine to provide rated thrust using engine sensors and also to protect the aircraft from unacceptable thrust or power changes on more than one engine due to faulty or erroneous aircraft signals.

Thrust and power command signals sent from aircraft are exempt from the requirement of §33.28(d). If the aircraft thrust or power command system is configured to move the engine thrust or power levers or transmit an electronic signal to command a thrust or power change, the engine control system merely responds to the command and changes engine thrust or power as appropriate. The engine control system may have no way of knowing that the sensed throttle or power lever movement was correct or erroneous.

In both the moving throttle (or power lever) and non-moving throttle (or power lever) configurations, it is the installer's responsibility to show that a proper functional hazard analysis is performed on the aircraft system involved in generating engine thrust or power commands, and that the system meets the appropriate aircraft's functional hazard assessment safety related requirements. This task is an aircraft certification issue.

(c) Design assessment

The applicant should evaluate the impact of the failure of aircraft-supplied data on the engine's output power or thrust characteristics throughout the flight envelope. The applicant should prepare a fault accommodation chart that defines the fault accommodation architecture for the aircraft-supplied data.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

There may be elements of the engine control system that are mounted in the aircraft and are not part of the engine type design, but which are dedicated to the engine control system and powered by it, such as a throttle position resolver. In these instances, such elements are considered to be an integral component of the electronic engine control system and are not considered aircraft data.

In the case where the particular failure modes of the aircraft air data may be unknown, the typical failure modes of (a) loss of data, and (b) erroneous data should be assumed. The term "erroneous data" is used herein to describe a condition where the data appears to be valid but is incorrect.

Such assumptions and the results of the evaluation of erroneous aircraft data should be provided to the installer.

(d) Examples of accommodation means

The followings are examples of possible accommodation means.

- Accommodation for loss of all aircraft-supplied data may be accomplished by providing an alternate control mode independent of aircraft-supplied data.

- Dual sources of aircraft-supplied sensor data with local engine sensors provided as voters and alternate data sources.

- Use of synthesized engine parameters as voters. When synthesized parameters are used for control or voting purposes, the analysis should consider the impact of temperature and other environmental effects on those sensors whose data are used in the synthesis. The variability of any data or information necessary to relate the data from the sensors used in the synthesis to the parameters being synthesized should also be assessed.

(e) Effects on the engine

§33.75 defines the hazardous engine effects.

§33.28(d) is primarily intended to address the effects of aircraft signals, such as aircraft air data information, or other signals which could be common to all engine control systems in a multi-engine installation. The control system design should ensure that the full-up system is capable of providing the declared minimum rated thrust or power through out the engine operation envelope.

..

§ 33.28(d)(1) requires the applicant to provide an analysis of the effect of loss or corruption of aircraft data on engine thrust or power. The following guidance applies to engine control systems for engines intended for applications on aircraft designed to meet Part 25 requirements. For applications other than those that must comply with Part 25 requirements, the engine applicant may justify to the FAA that a different change in power or thrust than those listed below may be acceptable.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

For fixed-wing multi-engined aircraft operating in the engine approved take-off envelope, erroneous data in aircraft signals used by the engine control system, should not be allowed to affect the power or thrust of each engine by more than 3%. When operating outside the engine's takeoff envelope but inside the engine's maximum continuous envelope erroneous aircraft data should not cause a thrust or power change greater than 10%. When operating outside the approved engine maximum continuous envelope, the effects of erroneous aircraft data on engine power or thrust may be allowed to increase with increasing altitude, but erroneous aircraft data should not be allowed to affect the power or thrust of each engine by more than 20%. Thrust or power changes greater than 10% should be included in the control system's LOTC analysis.

For multi-engined rotorcraft the power changes associated with the use of erroneous data should normally be less than 10% of takeoff power. If greater than 10%, they should be agreed with the certification authority.

(f) Validation

Functionality of the fault accommodation logic should be demonstrated by test. All fault accommodation modes for all control modes should be tested and evaluated.

If an alternate control mode independent of aircraft-supplied data has been provided to accommodate the loss of all aircraft-supplied data, sufficient testing should be conducted to demonstrate that the operability requirements have been met. Characteristics of operation in this mode should be included in the instructions for operating the engine.

13. AIRCRAFT SUPPLIED ELECTRICAL POWER

(a) Objective

Prior to the introduction of electrical/electronic technology, engine control systems were almost independent from the aircraft. For example, when dealing with aircraft situations like total electrical power failure, the flight crew did not have to be concerned about engine stability or operability, because the hydromechanical engine control system was independent from aircraft-supplied power. One of the objectives of §33.28 is to maintain this independence as far as practicable.

The engine control system should be designed and constructed so that after the engine is started and operating at or above idle, the engine will continue to function normally and without an "unacceptable effect on power or thrust or engine operating characteristics", in case of loss or interruption of aircraft-supplied electrical power at any point within the declared engine operating envelope.

(b) Analysis of the design architecture

An analysis and review of the design architecture should identify the requirements for dedicated electrical power sources and aircraft supplied power sources. The analysis should include the sources of power and the effects of loss or degradation of these sources. If the engine is

dependent on aircraft supplied power for any operational functions, the analysis should result in a definition of the requirements for aircraft supplied power.

The capacity of any engine dedicated power source which would be required for complying with §33.28 (e)(1) should provide sufficient margin to maintain confidence that the engine control system will continue to function in all anticipated engine operating conditions where the control system is designed and expected to recover engine operation in-flight. This margin should account for any other anticipated variations in the output of the dedicated power source such as those due to temperature variations, manufacturing tolerances and idle speed variations. The design margin should be substantiated by test and/or analysis and should also take into account any deterioration over the life of the engine.

In the case of rotorcraft, it is recognized that the engine control system may require aircraft power during ground operations.

When compliance with FAR 33.28(e)(1) imposes a dedicated electrical power source, failure of this source should be addressed in the LOTC analysis required under FAR 33.28(b)(1)(i). While no credit is normally given in the LOTC analysis for the use of aircraft-supplied electrical power as a backup power source, aircraft power has typically been provided for the purpose of accommodating the loss of the engine's dedicated power supply. However, LOTC allowance for the use of aircraft power as the power source for an engine control backup system would be reviewed on a case-by-case basis.

When aircraft electrical power is necessary for operation of the engine control system, §33.28(e)(3)requires that the engine instructions for installation contain the engine control system's electrical power supply quality requirements. This should include steady-state and transient under-voltage and over-voltage limits for the equipment. The power input requirements of DO-160 (rev. D), Section 16, are considered to provide an acceptable definition of such requirements. If DO-160 is used, any exceptions to the power quality requirements cited in DO-160 for the particular category of equipment specified, should be stated.

It is recognized that the electronic components of the engine control system may cease to operate during some low voltage aircraft power supply conditions beyond those required to sustain normal operation, but in no case should the operation of the engine control result in a hazardous engine condition as defined §33.75. In addition, low voltage transients outside the control system's declared capability should not cause permanent loss of function of the control system, or result in inappropriate control system operation which could cause the engine to exceed any operational limits, or cause the transmission of erroneous data.

When aircraft power recovers from a low-voltage condition to a condition within which the control is expected to operate normally, the engine control system should resume normal operation. The time interval associated with this recovery should be contained in the engine instructions for installation. It is recognized that aircraft power supply conditions may lead to an engine shutdown or engine condition which is not recoverable automatically. In these cases the engine should be capable of being restarted, and any special flight crew procedures for executing an engine restart during such conditions should be contained in the engine instructions for

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

operation. The acceptability of any non-recoverable engine operating conditions - as a result of these aircraft power supply conditions - will be determined at aircraft certification.

If aircraft-supplied battery power is required to meet an "all engine out" restart requirement, the analysis should result in a definition of the requirements for this aircraft-supplied power. In any application where aircraft electrical power is used to operate the engine control system, such as low engine speed in-flight re-starting conditions, the effects of any aircraft electrical bus-switching transients or power transients associated with application of electrical loads, which could cause an interruption in voltage or a decay in voltage below that level required for proper control functioning, should be considered.

In some system architectures, a dedicated power source may not be required and an aircraft-supplied electrical power supply may be acceptable as the sole source of power. An example is a system that consists of a primary electronic single channel and a full capability hydromechanical back-up system that is independent of electrical power. (A full capability hydromechanical control system is one that meets all FAR Part 33 requirements and is not dependent on aircraft power.) In this type of architecture, loss or interruption of aircraft-supplied power is accommodated by transferring control to the hydromechanical system. Such architectures should also consider the effects of aircraft electrical power bus switching and bus power decays on engine control system operation during in-flight engine re-starts as well as other conditions. Transition from the electronic to the hydromechanical control mode is addressed under FAR 33.28(a)(1)(ii).

(c) Electrical power sources:

A dedicated power source is defined herein as an electric power source providing electrical power generated and supplied solely for use by a single engine control system. They usually are alternators, mechanically driven by the engine or the transmission system of rotorcraft.

Batteries are considered an aircraft-supplied electrical power source (see definition in paragraph (5) of this AC) except in the case of engine applications for small general aviation aircraft (i.e., aircraft less than 6000 lbs. maximum takeoff gross weight). For such aircraft, a battery source dedicated solely to the engine control system may be accepted as a dedicated power source. In such installations, appropriate information for the installer should be provided including, for example, health status and maintenance requirements for the dedicated battery system.

(d) Effects on the engine

In the case of loss of aircraft supplied power, an unacceptable change in power or thrust is defined as any decrease or more than a 10% increase in Takeoff power or thrust.

Where loss of aircraft power results in a change in engine control mode, the control mode transition should meet requirements of §33.28(a)(1)(ii).

The loss of some engine control functions that rely upon aircraft-supplied electrical power may be acceptable. Acceptability is based on evaluation of the change in engine operating characteristics, current experience with similar designs, or the accommodation designed into the control system.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

Examples of these are :

- Engine start and ignition
- Thrust Reverser deployment
- Anti-Icing (engine probe heat)
- Fuel Shut-Off
- Overspeed Protection Systems
- Functions without safety significance that are primarily performance enhancement functions which, if inoperative, do not affect the safe operation of the engine.

(e) Validation

The applicant should demonstrate the effects of loss of aircraft-supplied electrical power by engine test, system validation test or bench test or combination thereof.

14. PROGRAMMED LOGIC DEVICES

The devices considered under §33.28 (h) are usually called Programmed Logic Devices. Because of the nature and complexity of systems containing digital logic, the Programmed Logic Devices should be developed using a structured development approach, commensurate with the hazard associated with failure or malfunction of the system in which the device is contained.

Programmed Logic Devices include Application Specific Integrated Circuits (ASIC) and Programmable Logic Devices (PLDs).

An ASIC is defined as any masked programmed integrated circuit that requires physical customization of the device die by an ASIC vendor. Gate array, cell based and custom designs are included as they involve some level of customization of the mask sets used in the fabrication of the devices.

A PLD is defined as any device that is purchased as an electronic part and altered to perform an application specific function. PLDs include, but are not limited to, Programmable Array Logic (PAL) devices, Programmable Logic Array (PLA) devices, General Array Logic (GAL) devices, Field Programmable Gate Array (FPGA) devices, and Electrically or Erasable Programmable Logic Devices (EPLD). Programmable Logic Devices typically require programming using software which is done in-house by the equipment manufacturer.

RTCA DO-254/ EUROCAE ED-80 which provides guidance for the criticality, failure condition categories and design assurance levels associated with Programmed Logic Devices development, is an acceptable means, but not the only means, for showing compliance with §33.28 (h).

For off-the-shelf equipment or modified equipment, service experience may be used in showing compliance to this guidance. This should be acceptable provided the worst case failure or malfunction of the device for the new installation is no more severe than that for the original installation of the same equipment on another application. Consideration should also be given to any significant differences related to environmental, operational or the category of the aircraft where the original system was installed and certified.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

15. SECTION (--) RECIPROCATING ENGINES.

TBD

(**NOTE**: The FAA has a SGAE activity that will issue AC33.28-2 dedicated to reciprocating engines because designs are in work and can not wait for this AC or the draft AC33.28-1. Hopefully this subsequently will be harmonized with the JAA activity on reciprocating engines.. However, the intent is to have the harmonized rule address SGAE as well.)

16. ENGINE, PROPELLER AND AIRCRAFT SYSTEMS INTEGRATION AND THE INTER-RELATION BETWEEN ENGINE, PROPELLER AND AIRCRAFT CERTIFICATION ACTIVITIES

(a) Integration Activities

(1) Aircraft Functions Integrated into the Engine Control System
This involves the integration of aircraft and propeller control functions (i.e., those that have traditionally not been considered engine control functions), into the electronic engine control (EEC) system's hardware and software. Examples of this involve thrust reverser controls, propeller speed governors, which govern speed by varying pitch, and ATTCS systems. Although the aircraft functions incorporated into the EEC system may receive review at engine certification, the acceptability of these functions would be determined at aircraft certification.

The EEC system may be configured to contain only part of the aircraft system's functionality, or it may contain virtually all of it. Thrust reverser control systems are an example where only part of the functionality is included in the EEC system. In such cases, the aircraft is configured to have separate switches and logic (i.e., independent from the EEC system) as part of the thrust reverser control system. This separation of reverser control system elements and logic provides an architectural means to limit the criticality of the functions provided by the EEC system.

However, in some cases the EEC system may be configured to incorporate virtually all of a critical aircraft function. Examples of this "virtually completeness" in aircraft functionality are EEC systems which contain full authority to govern propeller speed in turboprop powered aircraft and ATTCS systems in turbofan power aircraft. The first of these is considered critical because, if an engine fails, the logic in the engine control must be configured to feather the propeller on that engine. Failure to rapidly feather the propeller following an engine failure results in excessive drag on the aircraft, and such a condition can be critical to the aircraft. The second example, that of an ATTCS system, is considered critical because the system is required to increase the thrust

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

of the remaining engine(s) following an engine failure during takeoff, and the increased thrust on the remaining engines is necessary to achieve the required aircraft performance.

All of the above examples of integration involve aircraft functionality that would receive significant review during aircraft certification.

(2) Integration of Engine Control Functions into Aircraft Systems
The trend toward systems integration may lead to aircraft systems performing functions traditionally considered part of the engine control.

Some limited designs may have functions, traditionally considered part of the engine control system, provided by the aircraft, but the EEC system itself, which is part of the type design, provides all the functionally required to safely operate the engine in accordance with FAR 33, 35 and other applicable regulations. An example of such a "limited design" would be an engine control which receives a torque output demand signal from the aircraft and responds by changing the engine's fuel flow and other variables to meet that demand.

Other designs may use aircraft systems to implement a significant number of the engine control system functions. An example would be the complex integrated flight and engine control systems – integrated in aircraft avionics units - which govern engine speed, rotor speed, rotor pitch angle and rotor tilt angle in tilt-rotor aircraft

In all of these cases, the functions provided by the engine system which is part of the engine type design are certified with the engine and the completed system including both engine and aircraft provided functions are certified with the aircraft. Whenever possible, compliance to aircraft rules will be based on compliance with comparable engine rules. However, this is not always possible and in the end, the "airplane" including the "engine" must meet the "airplane" rules.

In these designs, aircraft systems may be an integral part of engine regulatory compliance. In such cases, the FAA considers the engine applicant to be responsible for specifying the requirements for the EEC system in the instruction for installation and substantiating the adequacy of those requirements. These requirements become part of the engine type design.

(b) Certification Activities

(1) Objective

To satisfy the aircraft requirements, such as FAR/JAR 25.901, 25.903 and 25.1309, an analysis of the consequences of failures of the engine control system on the aircraft has to be made. The engine manufacturer should, together with the aircraft manufacturer, ensure that the software levels and safety and reliability objectives for the engine electronic control system are consistent with these associated aircraft requirements.

Also, the use of the electronic technology has consistently resulted in greater integration of engine, propeller and aircraft systems. For example, in some applications the engine EEC unit may integrate the control functions for the propeller, or the aircraft computers may integrate the engine control and the propeller control functions.

There must be a clear definition of the respective certification tasks of the various applicants: engine, propeller and aircraft manufacturers, with the associated engine, propeller and aircraft certificating authorities.

(2) Interface Definition & System Responsibilities

System responsibilities as well as interface definitions should be identified for the functional and hardware and software aspects between the engine, propeller and the aircraft systems in the appropriate documents. It is recommended that these responsibilities be summarized in the various plans for engine, propeller and aircraft certification.

In particular, the engine/propeller/aircraft documents should cover:

(i) Functional requirements and criticality (which may be based on engine, propeller and aircraft considerations),

(ii) Fault accommodation strategies, and

(iii) Maintenance strategies

(iv) The software quality level (per function if necessary),

(v) The reliability objectives for –
--LOTC events
--Transmission of faulty parameters,

(vi) The environmental requirements including the degree of protection against lightning or other electromagnetic effects (e.g., level of induced voltages that can be supported at the interfaces),

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

In this example, the propeller functions and characteristics defined by the propeller manufacturer that are to be provided by the engine control system, would normally need to be refined by flight test. However, the propeller manufacturer is responsible for ensuring that these requirements that would be certificated as part of the engine certification program, although not refined by flight test, define an airworthy configuration. Definition of an airworthy configuration, although an unrefined configuration, is required because one of the essential requirements of a certificated engine is that it be airworthy.

-

- In addition, any type design changes to the engine control system which could affect the functioning of the propeller must be properly coordinated between the cognizant ACO's ,engine, and propeller manufacturers and vice versa, if applicable.

(ii) Case of an aircraft computer performing the functions for the control of the engine and/or the propeller. This example is not intended to provide a methodology that must be followed by the responsible aircraft and propeller parties involved. The intent is to provide an example of how these complex engine control systems with shared resources may be approached to reach agreement on responsibilities of the various parties involved with the certification process when the traditional approach to engine certification that includes an engine control system is not applicable.

- The aircraft certification would address all general requirements such as software quality assurance procedures, EMI/lightning protection levels.

- The aircraft certification would address the functional aspects for the aircraft functions.

- The engine certification would address the functional aspects for the engine functions (safety analysis, rate for LOTC events, effect of loss of aircraft supplied data, etc.) The fault accommodation logic affecting the control of the engine, for example, would be reviewed at that time.

- The propeller certification would address the functional aspects for the propeller control functions (safety analysis, contribution to LOTC events, effect of loss of aircraft supplied data, etc.) The fault accommodation logic affecting the control of the propeller, for example, would be reviewed at that time.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

(vii) Engine, propeller and aircraft interface data and characteristics, and

(viii) Aircraft electrical power supply requirements and characteristics (if relevant).

(3) Distribution of Compliance Tasks

The objective in any engine or propeller certification program should be to provide appropriate data that will provide evidence of compliance for both engine and aircraft requirements that are applicable to the engine control system. If anything done during engine or propeller certification is intended to also directly demonstrate or support compliance with an aircraft regulation, care should be taken that the installation effects and differences between the engine, propeller and aircraft requirements are clearly understood and accounted for. Also, the overall "aircraft certification plan" should clearly identify where this approach is being proposed. This would allow all parties to review and agree with the plan and assure that the necessary airplane information gets to the engine authority to facilitate an informed finding.

The aircraft certification plans should deal with the overall integration of the engine and propeller in compliance with the applicable aircraft requirements.

The engine and propeller certification plans should address the functional aspects of the engine and propeller control systems for compliance with the applicable engine and propeller control system requirements.

Two examples are given below to illustrate this principle.

(i) Case of an EEC unit performing the functions for the control of the engine and the functions for the control of the propeller:

- The engine certification would address all general requirements such as software quality assurance procedures, EMI/lightning protection levels, effects of loss of aircraft supplied power.

- The engine certification would address the functional aspects for the engine functions (safety analysis, rate for LOTC events, effect of loss of aircraft supplied data, etc.). The fault accommodation logic affecting the control of the engine, for example, will be reviewed at that time.

- The propeller certification would similarly address the functional aspects for the propeller control functions. The fault accommodation logic affecting the control of the propeller, for example, would be reviewed at that time.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.

End of file.

This document does not represent Final Agency Action on this matter, and shall not be viewed as a guarantee that any final action will follow in this or any other form.